bitdefender TOTAL SECURITY 2011

Manual do Utilizador

BitDefender Total Security 2011
Manual do Utilizador

Publicado 2010.08.09

Aviso Legal

Índice

Instalação e Remoção 1

1. Requisitos de Sistema 2
   1.1. Requisitos Minímos do Sistema 2
   1.2. Requisitos de sistema recomendados 2
   1.3. Requisitos de Software 2

2. A preparar a Instalação 4

3. Instalar BitDefender 5
   3.1. Passo 1 - Introdução 5
   3.2. Passo 2 - Preparar a Instalação 5
   3.3. Passo 3 - Registo 6
   3.4. Passo 4 - Escolher o Modo 9
   3.5. Passo 5 - Configurar 10
   3.6. Passo 6 - Opções de Suporte 15
   3.7. Passo 7 - Confirmar 15
   3.8. Passo 8 - Terminar 15

4. Fazer o Upgrade de Versões Anteriores do BitDefender 17

5. Remover ou Reparar o BitDefender 18

Introdução 19

6. Apresentação 20
   6.1. A abrir o BitDefender 20
   6.2. Icon da Barra de Tarefas 20
   6.3. Barra de Actividade da Análise 21
      6.3.1. Analisar Ficheiros e Pastas 22
      6.3.2. Desactivar/Restaurar Barra de Actividade da Análise 23
   6.4. Detecção Automática de Dispositivos 23

7. Janela Principal da Aplicação 25
   7.1. Modo Básico 25
      7.1.1. Estado da Área 26
      7.1.2. Área Proteja o seu PC 26
      7.1.3. Área de Ajuda 27
   7.2. Modo Intermédio 27
      7.2.1. Painel 28
      7.2.2. Segurança 29
      7.2.3. TUNE-UP 30
      7.2.4. Gestor de Ficheiros 31
      7.2.5. REDE 33
   7.3. Modo Avançado 33

8. Ferramentas 36

9. Alertas e Pop-ups 39

9.1. Alertas Antivírus . . . 39
9.2. Alertas do Controlo Activo de Vírus . . . 40
9.3. Alertas de Detecção de Dispositivo . . . 40
9.4. Pop-ups e Alertas da Firewall . . . 41
9.5. Alertas Antiphishing . . . 42
9.6. Mensagens de Alerta do Controlo Parental . . . 43
9.7. Alertas do Controlo de Privacidade . . . 43
9.7.1. Alertas de Registo . . . 43
9.7.2. Alertas de Script . . . 44
9.7.3. Alertas de Cookie . . . 44

10. Reparar Incidência . . . 45
10.1. Assistente Reparar Incidências . . . 45
10.2. Configurar os Alertas de Estado . . . 46

11. Configurar Definições Principais . . . 48
11.1. Opções de Segurança . . . 48
11.2. Definições de Alertas . . . 50
11.3. Configuração Geral . . . 51
11.4. Reconfigurar o Perfil de Utilização . . . 52

12. Histórico e Eventos . . . 54

13. Registo e a Minha Conta . . . 55
13.1. Registar BitDefender Total Security 2011 . . . 55
13.2. A activar o BitDefender . . . 56
13.3. Adquirir ou Renovar Chaves de Licença . . . 58

Configuração e Gestão . . . 59

14. Configuração Geral . . . 60

15. Protecção Antivírus . . . 64
15.1. Protecção em Tempo-real . . . 64
15.1.1. Ajustar o Nível de Protecção em Tempo Real . . . 65
15.1.2. Criar um Nível de Protecção Personalizado . . . 66
15.1.3. Alterar as Acções Aplicadas aos Ficheiros Detectados . . . 67
15.1.4. Restaurar as Predefinições . . . 68
15.1.5. Configurar o Controlo Activo de Vírus . . . 69
15.1.6. Configurar o Sistema de Detecção de Intrusão: . . . 71
15.2. Análise a-pedido . . . 71
15.2.1. Analisar Ficheiros e Pastas . . . 72
15.2.2. Assistente de Análise Antivírus . . . 73
15.2.3. Ver os Relatórios da Análise . . . 76
15.2.4. Gerir Tarefas de Análise Existentes . . . 76
15.3. Configurar Exclusões da Análise . . . 83
15.3.1. Excluir Ficheiros ou Pastas da Análise . . . 84
15.3.2. Excluir Extensões de Ficheiros da Análise . . . 85
15.3.3. Gerir Exclusões da Análise . . . 86
15.4. Àrea de Quarentena . . . 86

16. Protecção Antiphishing . . . 89

16.1. Configurar a Lista Branca de Antiphishing . . . 89
16.2. Gerir a Protecção Antiphishing do BitDefender no Internet Explorer e Firefox . . . 89

17. Consultor de Procura . . . 91
17.1. Desactivar o Consultor de Procura: . . . 91

18. Antispam . . . 92
18.1. Compreender o Antispam . . . 92
18.1.1. Filtros Antispam . . . 92
18.1.2. Operação Antispam . . . 94
18.1.3. Actualização do Antispam . . . 95
18.2. Assistente de Optimização Antispam . . . 96
18.3. Utilizar a Barra de Ferramentas Antispam na Janela do Seu Cliente de Correio Electrónico . . . 97
18.3.1. Indicar os Erros de Detecção . . . 99
18.3.2. Indicar Mensagens de Spam Não Detectadas . . . 99
18.3.3. Retreinar o Motor de Aprendizagem (Bayesiano) . . . 99
18.3.4. Guardar e Carregar a Base de Dados Bayesiana . . . 100
18.3.5. Configurações Gerais . . . 100
18.4. Ajustar o Nível de Protecção . . . 101
18.5. Configurar a Lista de Amigos . . . 101
18.6. Configurar a lista de Spammers . . . 102
18.7. Configurar os Filtros e as Definições do Antispam . . . 104

19. Controlo Parental . . . 106
19.1. Configurar Controlo Parental . . . 106
19.1.1. Proteger as Definições do Controlo Parental . . . 108
19.1.2. Controlo Web . . . 109
19.1.3. Controlo de Aplicação . . . 111
19.1.4. Controlo de Palavras-Chave . . . 112
19.1.5. Controlo de Mensagens Instântaneas (IM) . . . 114
19.2. Monotorizar Actividade das Crianças . . . 115
19.2.1. Consultar os Relatórios do Controlo Parental . . . 115
19.2.2. A Configurar Notificações de E-mail . . . 116
19.3. Controlo Parental Remoto . . . 118
19.3.1. Pré-Requisitos para Utilizar o Controlo Parental Remoto . . . 118
19.3.2. Activar o Controlo Parental Remoto . . . 118
19.3.3. Aceder ao Controlo Parental Remoto . . . 119
19.3.4. Monitorizar as Actividades dos Seus Filhos à Distância . . . 119
19.3.5. Alterar as Definições do Controlo Parental à Distância . . . 120

20. Controlo de Privacidade . . . 123
20.1. Configurar Nível de Protecção . . . 123
20.2. Controlo de identidade . . . 124
20.2.1. Sobre o Controlo de Identidade . . . 124
20.2.2. Configurar o Controlo de Identidade . . . 125
20.2.3. Gerir Regras . . . 128
20.3. Controlo de registo . . . 128
20.4. Controlo de cookies . . . 129
20.5. Controlo de script . . . 130

21. Firewall 132
21.1. Definições da Protecção 132
21.1.1. Definir a Acção por Defeito 132
21.1.2. Configuração Avançada da Firewall 133
21.2. Regras de Acesso a Aplicações 134
21.2.1. Ver Regras Actuais 134
21.2.2. Adicionar Regras Automaticamente 136
21.2.3. Adicionar Regras Manualmente 136
21.2.4. Gestão Avançada de Regras 139
21.2.5. Apagar e Redifinir Regras 140
21.3. Definições de Rede 140
21.3.1. Zonas de Rede 141
21.4. Dispositivos 142
21.5. Controlo de Ligação 143
21.6. Resolver Problemas com a Firewall 143
22. Vulnerabilidade 145
22.1. A analisar em busca de Vulnerabilidades 145
22.2. Estado 146
22.3. Definições 146
23. Backup 148
23.1. Fazer o Backup Local de Dados 148
23.2. Restaurar Dados de Backup Local 150
23.3. Definições de Backup 151
23.3.1. Iniciação 151
23.3.2. Admin de Tarefas 152
23.3.3. Visualizador de Relatórios 166
23.3.4. Caixa de Ferramentas 168
23.3.5. Barra de Menu 169
24. Encriptação de Chat 172
24.1. Desactivar a Encriptação para Utilizadores Específicos 173
24.2. Barra de Ferramentas do BitDefender na Janela de Conversação 173
25. Encriptação Ficheiro 174
25.1. Gerir Cofres de Ficheiros no Interface do BitDefender 174
25.1.1. Criar Cofre 174
25.1.2. Abrir Cofre 175
25.1.3. Fechar Cofre 176
25.1.4. Alterar Palavra-passe do Cofre 177
25.1.5. Adicionar Ficheiros ao Cofre 177
25.1.6. Remover os ficheiros do Cofre 178
25.1.7. Ver Conteúdo do Cofre 179
25.1.8. Eliminar Cofre de Ficheiros 180
25.2. Gerir Cofres de Ficheiros no Windows 180
25.2.1. Criar Cofre 181
25.2.2. Abrir Cofre 182
25.2.3. Fechar Cofre 182
25.2.4. Adicionar ao Cofre de Ficheiros 183
25.2.5. Remover do Cofre de Ficheiros 183

25.2.6. Alterar Palavra-passe do Cofre 184
26. TUNE-UP 185
26.1. Desfragmentar Volumes de Discos Duros 185
26.2. Limpar o Seu PC 186
26.3. Apagar Ficheiros Permanentemente 187
26.4. Limpar o Registo do Windows 188
26.5. Recuperar Limpeza de Registo 190
26.6. Localizar Ficheiros Duplicados 190
26.7. Monitor de Desempenho 191
27. Modo de Jogo / Portátil 193
27.1. Modo de Jogo 193
27.1.1. Configurar Modo de Jogo Automático 194
27.1.2. Gerir a Lista de Jogos 194
27.1.3. Adicionar ou Editar Jogos 195
27.1.4. Configurar as Definições do Modo de Jogo 195
27.1.5. Mudar a Tecla de Atalho do Modo de Jogo 196
27.2. Modo Portátil 196
27.2.1. Configurar Definições do Modo de Portátil 196
27.3. Modo Silêncio 197
27.3.1. Configurar a Acção em Ecrã Completo 198
27.3.2. Configurar as Definições do Modo Silêncio 198
28. A Sua Rede 199
28.1. Activar a Rede BitDefender 199
28.2. Adicionar Computadores à Rede BitDefender 200
28.3. Gerir a Rede BitDefender 200
29. Actualização 203
29.1. Efectuar uma Actualização 204
29.2. Configurar Definições de Actualização 204
29.2.1. Configuração da Localização da Actualização 205
29.2.2. Configurar Actualização Automática 205
29.2.3. Configurar Actualização Manual 206
29.2.4. Configuração Avançada 206
Como 207
30. Como Posso Analisar Ficheiros e Pastas? 208
30.1. Usar o Menu Contextual do Windows 208
30.2. Usar Tarefas de Análise 208
30.3. Usando a Barra de Actividade da Análise 209
31. Como Posso Criar Uma Tarefa de Análise Personalizada? 211
32. Como Posso Agendar uma Análise ao Computador? 213
33. Como Posso Fazer Cópias de Segurança? 215
34. Como Posso Restaurar os Dados da Cópia de Segurança? 217
35. Como Posso Criar Contas de Utilizador do Windows? 218

36. Como Posso Actualizar o BitDefender Através de um Proxy? ... 219
37. Como Posso Fazer o Upgrade para Outro Produto do BitDefender 2011? ... 220
38. Como Posso Melhorar a Velocidade do Meu Sistema? ... 221
39. Como Posso Utilizar Cofres de Ficheiros? ... 222

Troubleshooting e Obter Ajuda ... 224

40. Solução de problemas ... 225
40.1. Problemas de Instalação ... 225
40.1.1. Erros de Validação da Instalação ... 225
40.1.2. Falha na Instalação ... 226
40.2. O meu sistema parece estar lento ... 227
40.3. A Análise Não Inicia ... 228
40.4. Já Não Consigo Utilizar uma Aplicação ... 229
40.5. Não Consigo Ligar à Internet ... 230
40.6. Não Consigo Usar Uma Impressora ... 230
40.7. Não Consigo Partilhar Ficheiros Com Outro Computador ... 232
40.8. A minha Internet está lenta ... 233
40.9. Como Actualizar o BitDefender numa Ligação à Internet Lenta ... 234
40.10. O Meu Computador Não Está Ligado à Internet. Como Posso Actualizar o BitDefender? ... 234
40.11. Os serviços BitDefender não estão a responder ... 235
40.12. O Filtro Antispam Não Está a Funcionar Correctamente ... 235
40.12.1. Mensagens Legítimas são marcadas como [spam] ... 236
40.12.2. Muitas Mensagens de Spam Não São Detectadas ... 239
40.12.3. O Filtro Antispam Não Detecta Nenhuma Mensagem Spam ... 241
40.13. A Desinstalação do BitDefender Falhou ... 242

41. Remover Malware do Sistema ... 244
41.1. CD de Emergência BitDefender ... 244
41.2. O Que Fazer Se o BitDefender Encontrar Vírus No Seu Computador? ... 245
41.3. Como Posso Limpar o Vírus de um Arquivo? ... 246
41.4. Como Posso Limpar o Vírus de um Arquivo de Correio Electrónico? ... 247
41.5. Como Posso Analisar o Computador no Modo de Segurança? ... 248
41.6. O Que Fazer Se o BitDefender Identificou um Ficheiro Limpo como Infectado? ... 249
41.7. Como Limpar os Ficheiros Infectados da Informação de Volume de Sistema ... 249
41.8. O que são Ficheiros Protegidos por Palavra-Passe no Relatório de Análise? ... 251
41.9. O Que São os Itens Ignorados no Relatório de Análise? ... 251
41.10. O que são os Ficheiros Sobre-Comprimidos no Relatório de Análise? ... 251
41.11. Porque é que o BitDefender eliminou automaticamente um ficheiro infectado? ... 251

42. Apoio ... 253
42.1. Recursos Em Linha ... 253

42.1.1. Base de Conhecimento do BitDefender 253
42.1.2. Fórum de Suporte BitDefender 253
42.1.3. Portal Malware City 254
42.1.4. Tutoriais 254
42.2. Pedir Ajuda 255

43. Contactos 257
43.1. Endereços Web 257
43.2. Distribuidores Locais 257
43.3. Escritórios BitDefender 258

44. Informações Úteis 260
44.1. Como Posso Remover Outras Soluções de Segurança? 260
44.2. Como Posso Reiniciar no Modo de Segurança? 261
44.3. Estou a Utilizar uma Versão de 32 ou 64 Bit do Windows? 261
44.4. Como Posso Encontrar as Minhas Definições de Proxy? 262
44.5. Como Posso Remover Totalmente o BitDefender? 262
44.6. Como Posso Activar/Desactivar a Protecção Em Tempo Real 262
44.7. Como Posso Mostrar Objectos Ocultos no Windows? 263

Glossário 264

Instalação e Remoção

1. Requisitos de Sistema

Só pode instalar o BitDefender Total Security 2011 nos computadores que tenham os seguintes sistemas operativos:

- Windows XP com Service Pack 3 (32 bit) / Windows XP com Service Pack 2 (64 bit)
- Windows Vista com Service Pack 1 ou superior (32/64 bit)
- Windows 7 (32/64 bit)

Antes da instalação, certifique-se que o seu computador cumpre com os requisitos mínimos de hardware e software.

Nota

Para ficar a saber que sistemo operativo o seu computador contém e a informação de hardware do mesmo, clique com o botão direito do rato no ícone **Meu Computador** no Ambiente de Trabalho e depois seleccione **Propriedades** do menu.

1.1. Requisitos Minímos do Sistema

- 1 GB de espaço disponível em disco
- Processador de 800 MHz
- Memória RAM:
  - 512 MB para o Windows XP
  - 1 GB para o Windows Vista e Windows 7
- Internet Explorer 6.0
- .NET Framework 2 (também disponível no kit de instalação)
- Adobe Flash Player 10.0.45.2

1.2. Requisitos de sistema recomendados

- 1 GB de espaço disponível em disco
- Processador Intel Core Duo (1,66 GHz) ou equivalente
- Memória RAM:
  - 1 GB para o Windows XP e Windows 7
  - 1.5 GB para Windows Vista
- Internet Explorer 7
- .NET Framework 2 (também disponível no kit de instalação)
- Adobe Flash Player 10.0.45.2

1.3. Requisitos de Software

A protecção antiphising está disponível apenas para:

- Internet Explorer 6.0 ou superior
- Mozilla Firefox 3.x
- Yahoo! Messenger 8.1

- Microsoft Windows Live Messenger 8

Encriptação para Instant Messaging (IM) está disponível para:

- Yahoo! Messenger 8.1
- Microsoft Windows Live Messenger 8

A protecção Antispam é fornecida para todos os clientes de e-mail POP3/SMTP.No entanto a barra de ferramentas do Antispam BitDefender apenas se integra em:

- Microsoft Outlook 2003 / 2007 / 2010
- Microsoft Outlook Express
- Microsoft Windows Mail
- Mozilla Thunderbird 3.0.4

2. A preparar a Instalação

Antes de instalar o BitDefender Antivírus 2010, complete estes procedimentos para assegurar uma boa instalação:

- Assegure-se que o computador onde vai instalar o BitDefender contém os requisitos minimos do sistema.Se o seu computador não contém os requisitos mínimos do sistema, o BitDefender não será instalado ou, se instalado, não trabalhará correctamente e provocará lentidão e instabilidade no sistema.Para ver a lista completa dos requisitos mínimos do sistema, por favor consulte o “*Requisitos de Sistema*” (p. 2).
- Ligue-se ao computador utilizando uma conta de Administrador.
- Remova quaisquer outros softwares de segurança do seu computador.Executar dois programas de segurança simultaneamente poderá afectar o seu funcionamento e causar grandes problemas no sistema.Por defeito, o Windows Defender será desactivado antes da instalação começar.
- Desativar ou remover qualquer programa de firewall que possam estar em execução no computer.Executar dois programas de firewall simultaneamente poderá afectar o seu funcionamento e causar grandes problemas no sistema.Por defeito, a Firewall do Windows será desactivada antes da instalação começar.

3. Instalar BitDefender

Pode instalar o BitDefender a partir do CD de instalação do BitDefender ou utilizando o ficheiro de instalação descarregado do site da BitDefender ou de outros sites autorizados (por exemplo, de sites de parceiros da BitDefender ou de uma loja on-line).Pode descarregar o ficheiro de instalação do site da BitDefender seguindo este endereço: http://www.bitdefender.com/site/Downloads/.

- Para instalar o BitDefender a partir do CD, insira o CD na drive. Uma janela de boas-vindas aparecerá em alguns momentos. Siga as instrucções e começe a instalação.

Nota

O écran de boas-vindas dá-lhe a opção de copiar o pacote de instalação do CD para uma pen USB. Isto é útil se necessitar de instalar o BitDefender num computador que não tem uma drive de CD (por exemplo um netbook).Insira a pen USB na drive respectiva e depois clique em **Copiar para a USB**.Depois, vá até ao computador sem a drive de CD, insira a pen USB e faça duplo-clique no ficheiro `runsetup.exe` que se encontra na pasta onde guardou o pacote de instalação.

Se o ecrã de boas-vindas não aparecer, vá ao directório-raiz do CD e faça duplo clique em `autorun.exe`.

- Para instalar o BitDefender utilizando um ficheiro de instalação descarregado, localize o ficheiro e faça duplo-clique sobre ele.

O instalador irá primeiro verificar o seu sistema para validar a instalação.Se a instalação for válida, ser-lhe-á pedido que seleccione o idioma antes de aparecer o assistente de configuração.

O assistente vai ajudar a instalar o BitDefender no seu computador e, ao mesmo tempo, vai permitir-lhe configurar as definições principais e o interface de utilizador.

3.1. Passo 1 - Introdução

Por favor, leia o Acordo de Licença e seleccione **Ao assinalar esta caixa, acito o cordo de licença do BitDefender**.Clique em **Seguinte** para continuar.

Se não concordar com estes termos clique em **Cancelar**. O processo de instalação será cancelado e terminará.

3.2. Passo 2 - Preparar a Instalação

O BitDefender analisa o seu sistema e verifica se há outro software de segurança instalado.

Análise Rápida

É efectuada uma análise rápida às áreas críticas do seu sistema para garantir que não existe malware activo.

A análise não deverá demorar mais do que alguns minutos. Pode cancelá-la em qualquer momento clicando no respectivo botão.

Importante

É altamente recomendado que aguarde a conclusão da análise.
O malware activo pode interromper a instalação e causar a falha.

Depois de a análise terminar, os resultados são apresentados. Se for encontrada alguma ameaça, siga as instruções para a remover antes de continuar a instalação.

Clique em **Seguinte** para continuar.

Remover Software de Segurança Existente

O BitDefender Total Security 2011 avisa-o se tiver outros produtos de segurança instalados no seu computador.Clique no botão respectivo para iniciar o processo de desinstalação e siga as instruções para remover os produtos detectados.

Atenção

É altamente recomendável que desinstale qualquer outro antivírus detectado antes de instalar BitDefender. Usar dois ou mais produtos antivírus ao mesmo tempo num computador pode bloquear totalmente o seu sistema.

O BitDefender também recomenda acções a aplicar sobre recursos de segurança do Windows activados.

- **Desligar a Firewall do Windows** - para desligar a Firewall do Windows.

Importante

Recomendamos que desligue a Firewall do Windows uma vez que o BitDefender Total Security 2011 já inclui uma firewall avançada. Executar 2 firewalls no mesmo computador poderá causar problemas.

- **Desactivar o Windows Defender** - para desactivar o Windows Defender.

Clique em **Seguinte** para continuar.

3.3. Passo 3 - Registo

O processo de registo do BitDefender consiste em registar o produto com uma chave de licença e activar os recursos em linha criando uma conta BitDefender.

Registar o seu produto

Proceda consoante a sua situação:

- **Comprei o BitDefender Total Security 2011 num CD ou em linha**

  Neste caso, tem de registar o produto:

  1. Insira a chave de licença no campo de edição.

     Nota
     Pode encontrar a sua chave de licença:
     ▶ Na bolsa do CD.
     ▶ ou no cartão de registo do produto.
     ▶ no e-mail da sua compra on-line.
     Se não possuir uma chave de licença BitDefender, clique no link que lhe facultamos para ir até à loja on-line do BitDefender e adquirir uma.

  2. Clique em **Registar Agora**.
  3. Clique **Seguinte**.

- **Transferi o BitDefender Total Security 2011 para avaliação**

  Neste caso, pode utilizar todos os recursos do programa durante 30 dias.Para iniciar o período de avaliação, seleccione **Quero avaliar o BitDefender Total Security 2011 durante 30 dias** e clique em **Seguinte**.

Activar Recursos Online

TEM de criar uma conta BitDefender de forma a poder receber as actualizações do mesmo.A conta BitDefender também lhe dá acesso ao controlo parental em linha, a apoio técnico gratuito e a ofertas promocionais especiais.Se perder a sua chave de licença do BitDefender, pode entrar na sua conta em http://myaccount.bitdefender.com e recuperá-la.

Se não deseja criar uma conta BitDefender neste momento, seleccione **Criar Conta Mais Tarde** e clique em **Seguinte**.

Nota
Se estiver a instalar o BitDefender Total Security 2011 para avaliação, tem de criar uma conta BitDefender agora.
Se adquiriu o produto, tem de criar uma conta no prazo de 30 dias após a instalação.

De outra forma, actue de acordo com a sua presente situação:

- **Não tenho uma conta BitDefender**

  Para criar uma conta BitDefender com sucesso, siga estes passos:

  1. Seleccione **Criar uma nova conta**.

2. Digite as informações solicitadas nos campos correspondentes.Os dados que nos fornecer serão mantidos confidenciais.
   - **Nome de utilizador** - insira o seu endereço electrónico.
   - **Palavra-passe** - insira uma palavra-passe para a sua conta BitDefender.A palavra-passe tem de ter entre 6 e 16 caracteres de tamanho.
   - **Re-inserir a palavra-passe** - inserir novamente a palavra-passe previamente definida.

     Não tem de escrever novamente a palavra-passe se seleccionar não ocultar a palavra-passe enquanto escreve.

Nota
Uma vez com a conta activada, poderá utilizar o endereço de e-mail fornecido e a palavra-passe para entrar na sua conta em http://myaccount.bitdefender.com.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta.Clique em **Ver Opções de Contacto** e seleccione uma das opções disponíveis na janela que aparece.
   - **Envie-me todas as mensagens**
   - **Enviar mensagens importantes**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Submeter**.
5. Clique em **Seguinte** para continuar.

Nota
Antes de usar a sua conta, tem de a activar.
Verifique o seu e-mail e siga as instrucções da mensagem de e-mail que o serviço de registo BitDefender lhe enviou.

- **Já tenho uma conta BitDefender**

O BitDefender detectará automaticamente se já registou previamente uma conta BitDefender no seu computador.Nesse caso, forneça a palavra-passe da sua conta e clique em **Submeter**.Clique em **Seguinte** para continuar.

Se já tiver uma conta activada mas o BitDefender não a detecta, siga estes passos para registar essa conta ao produto:

1. Seleccione **Entrar (Conta Existente)**.
2. Digite o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes.

Nota
Se não se lembra da sua palavra-passe, clique em **Esqueceu a sua palavra-passe?** e siga as instruções.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta.Clique em **Ver Opções de Contacto** e seleccione uma das opções disponíveis na janela que aparece.
   - **Envie-me todas as mensagens**
   - **Enviar mensagens importantes**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Submeter**.
5. Clique em **Seguinte** para continuar.

3.4. Passo 4 - Escolher o Modo

Aqui pode escolher o tipo de instalação a efectuar e o modo do interface a utilizar.

Escolher o Tipo de Configuração

Estão disponíveis as seguintes opções de configuração:

- **Configuração Fácil** - seleccione esta opção se preferir uma instalação rápida e se não pretender configurar as definições do BitDefender em pormenor.
- **Configuração Personalizada** - seleccione esta opção se preferir personalizar a instalação e as definições do BitDefender.

Para ver um tutorial de ajuda com a instalação, clique em **Obter Ajuda**

Nota
Para instalar o BitDefender com uma configuração predefinida e avançar directamente para o último passo do assistente de instalação, seleccione **Saltar Configuração**.

Clique em **Seguinte** para continuar.

Escolher Localização da Configuração

Nota
Este passo só aparece se tiver escolhido uma **Configuração Personalizada**.

Por defeito, BitDefender Total Security 2011 será instalado em `C:\Programas\BitDefender\`.Se deseja alterar este caminho de instalação, clique em **Explorar** e seleccione a pasta na qual pretende que o BitDefender seja instalado.

Pode partilhar os ficheiros e as assinaturas com outros utilizadores do BitDefender.Desta forma, as actualizações do BitDefender são mais rápidas.Se não quiser activar este recurso, seleccione a respectiva caixa.

Nota

Não será partilhada qualquer informação de identificação pessoal se este recurso estiver activado.

Clique em **Seguinte** para continuar.

Escolher o Interface de Utilizador

Seleccione o modo do interface do utilizador que melhor se adequa às suas necessidades.BitDefender Total Security 2011 dá-lhe a possibilidade de escolher entre três interfaces, cada um concebido de acordo com as necessidades de diferentes utilizadores.

Modo Básico

Indicado para principiantes em computadores e pessoas que querem que o BitDefender proteja o seu computador e dados sem incómodos. Este modo é simples de usar e requer a mínima interacção da sua parte.

Tudo o que tem de fazer é reparar as incidências indicadas pelo BitDefender. Um assistente de passo-a-passo intuitivo ajudá-lo-á a resolver essas incidências.Adicionalmente, pode levar a cabo tarefas comuns, tais como actualizar as assinaturas de vírus e os ficheiros do BitDefender ou analisar o computador.

Modo Intermédio

Pode configurar as definições principais do BitDefender, corrija os problemas separadamente, gira os produtos do BitDefender instalados nos computadores da sua rede e escolha os problemas a monitorizar.Além disso, pode controlar o modo como os seus filhos usam o computador e a Internet configurando o Controlo Parental.

Modo Avançado

Adequado para os utilizadores com mais conhecimentos tecnicos, este modo permite-lhe configurar completamente cada funcionalidade do BitDefender.Também pode usar todas as tarefas disponiveis para proteger o seu computador e dados.

Faça a sua selecção e clique em **Seguinte** para continuar.

3.5. Passo 5 - Configurar

Aqui pode personalizar o seu produto.

Configurar Definições

Nota
Este passo só aparece se tiver definido o **Modo Avançado** do BitDefender.

Aqui pode activar/desactivar os recursos do BitDefender, organizados em duas categorias.Para alterar o estado de uma definição, clique no respectivo interruptor.

- **Opções de Segurança**

  Aqui, pode activar ou desactivar configurações do produto que abrangem diversos aspectos da segurança do computador e dos dados.

Definições	Descrição
Antivírus	A protecção em tempo-real assegura que todos os ficheiros acedidos por si ou por uma aplicação são analisados.
Actualização Automática	A actualização automática assegura que os produtos e as assinaturas mais recentes da BitDefender são descarregados da Internet e instalados automaticamente numa base regular.
Analisar Vulnerabilidades	A Verificação Automática de Vulnerabilidades assegura que o software crucial no seu PC está actualizado.
Antispam	O Antispam filtra as mensagens de E-mail recebidas, marcando a publicidade não solicitada e o lixo electronico como SPAM.
Antiphishing	A protecção Antiphishing web em tempo-real detecta e alerta-o em tempo-real se uma página web está feita para roubar informação pessoal.
Controlo de identidade	O Controlo de Identidade ajuda a impedir que os seus dados pessoais sejam expostos na Internet sem o seu consentimento. Bloqueia todas as mensagens instantâneas, mensagens de e-mail ou outras formas de transmissão de dados pela web que tenha definido como sendo privado para destinatários não autorizados (endereços).
Encriptação de Chat	A Encriptação de Conversa através do Yahoo! Messenger e Windows Live Messenger só é possível se a pessoa de contacto utilizar um produto BitDefender compativel.

Definições	Descrição
Controlo Parental	O Controlo Parental restringe o computador e as actividades online das crianças, baseado nas regras que você definiu.As restrições podem incluir o bloqueio de sites de web inadequados, bem como limitar o acesso à Internet e a jogos a um determinado horário.
Firewall	A Firewall protege o seu computador contra os hackers e os ataques maliciosos externos.
Encriptação Ficheiro	O Cofre de ficheiros mantém os seus documentos privados ao encriptá-los em drives de cofre especiais.Se desactivar o Cofre de Ficheiros, todos os cofres de ficheiros serão fechados e não será mais capaz de aceder aos ficheiros que eles contêm.

- **Configuração Geral**

Aqui, pode activar ou desactivar as definições referentes ao produto e à experiencia do utilizador.

Definições	Descrição
Modo de Jogo	O Modo de Jogo modifica temporariamente as definições de segurança de forma a minimizar o seu impacto no desempenho do seu sistema durante o jogo.
Detecção de Modo Portátil	O Modo Portátil modifica temporariamente as definições de segurança de forma a minimizar o seu impacto sobre o tempo de vida da bateria do seu portátil.
Definição de Palavra-passe	Isto assegura que as definições do BitDefender só podem ser modificadas pela pessoa que conhece esta palavra-passe. Quando activar esta opção, será solicitado a configurar as definições de palavra-passe.Insira a palavra-passe desejada nos dois campos e clique em **OK** para definir a palavra-passe.
Notícias BitDefender	Ao activar esta opção, irá receber notícias importantes sobre a empresa BitDefender, sobre as actualizações do produto ou sobre novas ameaças de segurança.

Definições	Descrição
Alertas de Notificação do Produto	Ao activar esta opção, irá receber alertas de informação.
Barra de Actividade da Análise	A barra de actividade da análise é uma janela pequena, transparente, que indica o progresso da actividade da análise do BitDefender.Para mais informação, por favor consulte o *"Barra de Actividade da Análise"* (p. 21).
Enviar relatórios de vírus	Ao activar esta opção, os relatórios das análises são enviados para o Laboratório BitDefender para análise. Estes relatórios não contém qualquer informação considerada pessoal e confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial.
Detecção de Surtos	Ao activar esta opção, os relatórios relativos a potenciais surtos de vírus são enviados para o Laboratório BitDefender para análise. Estes relatórios não contém qualquer informação considerada pessoal e confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial.

Clique em **Seguinte** para continuar.

Configurar as Ferramentas

Nota

Este passo só aparece se tiver definido o **Modo Básico** or **Modo Intermédio** do BitDefender.

Com os **Meus Instrumentos**, pode personalizar o painel de instrumentos adicionando atalhos para os recursos que são mais importantes para si.Desta forma, pode garantir o fácil acesso a eles.

Neste ecrã, pode adicionar atalhos para qualquer um dos seguintes instrumentos:

- Controlo Parental - controle e monitorize as actividades dos seus filhos no computador.
- Modo Jogo - configure o BitDefender para impedir que este interfira com o seu jogo.
- Modo Portátil - modifica temporariamente as definições da protecção para minimizar o impacto na duração da bateria do seu portátil.

- Gestão da rede Doméstica - gere os produtos BitDefender instalados na rede doméstica a partir de um único computador.

Seleccione os instrumentos que pretende adicionar e clique em **Seguinte** para continuar.

Configurar o Controlo Parental

Nota
Este passo só aparece se tiver adicionado o Controlo Parental aos Meus Instrumentos.

Pode seleccionar uma das três opções:

- **Definir o Controlo Parental nas contas dos filhos**

  Seleccione esta opção para activar o Controlo Parental nas contas do Windows criadas para os seus filhos e gerir a partir da conta de administrador.

- **Definir o Controlo Parental na conta actual**

  Seleccione esta opção para activar o Controlo Parental na conta do Windows actual. Isto significa que não terá de criar contas separadas para os seus filhos, mas as regras do Controlo Parental irão afectar todas as pessoas que utilizem esta conta.

  Neste caso, é necessária uma palavra-passe para proteger as definições do Controlo Parental.Pode definir agora ou mais tarde a partir da janela do BitDefender.

- **Saltar a configuração por agora**

  Seleccione esta opção para configurar este recurso mais tarde na janela do BitDefender.

Clique em **Seguinte** para continuar.

Gestão da Rede Pessoal

Nota
Este passo só aparece se tiver adicionado a Gestão de Rede Doméstica aos Meus Instrumentos.

Pode seleccionar uma das três opções:

- **Definir este PC como Servidor**

  Seleccione esta opção se pretende gerir os produtos BitDefender noutros computadores da rede doméstica a partir deste.

  É necessária uma palavra-passe para entrar na rede.Introduza nas respectivas caixas de texto e clique em **Submeter**.

- **Definir este PC como Cliente**

  Seleccione esta opção se o BitDefender será gerido a partir de outro computador da rede doméstica que também tem o BitDefender instalado.

  É necessária uma palavra-passe para entrar na rede.Introduza nas respectivas caixas de texto e clique em **Submeter**.

- **Saltar a configuração por agora**

  Seleccione esta opção para configurar este recurso mais tarde na janela do BitDefender.

Clique em **Seguinte** para continuar.

3.6. Passo 6 - Opções de Suporte

Aqui pode personalizar as opções de ajuda e suporte:

- Activar / desactivar as **Dicas Inteligentes**.As Dicas Inteligentes são mensagens personalizadas apresentadas no Painel de Instrumentos do BitDefender para o ajudar a melhorar o desempenho do seu computador.
- Confirme o endereço electrónico que irá utilizar se tiver de contactar o Apoio ao Cliente do BitDefender. Se não pretender contactar o Apoio ao Cliente por correio electrónico, seleccione a caixa respectiva.

3.7. Passo 7 - Confirmar

Aqui pode rever a configuração seleccionada.

Por defeito, também são agendadas duas tarefas:

- É agendada uma análise minuciosa ao sistema imediatamente após a conclusão da instalação.

  É recomendado que realize esta análise profunda para detectar todas as ameaças de malware presentes no seu sistema.

- Um análise ao sistema foi agendada para ser executada aos Domingos, às 2h.

  É vivamente recomendado que analise o seu sistema pelo menos uma vez por semana.Seleccione um dia e uma hora diferentes se a altura predefinida não for conveniente para si.Se o computador estiver desligado durante o momento do agendamento, a análise será levada a cabo da próxima vez que iniciar o seu computador.

Clique em **Terminar**.

3.8. Passo 8 - Terminar

A instalação está, agora, perto da conclusão. As definições finais são aplicadas e é efectuada uma actualização.

O assistente vai ser automaticamente encerrado no final da instalação.Se a opção foi seleccionada no passo anterior, será iniciada uma análise minuciosa ao sistema.

O assistente de configuração vai detectar a rede a que está ligado e irá permitir que a classifique como Casa/Escritório ou Pública.

Nota
Poderá ser necessário reiniciar o sistema.

4. Fazer o Upgrade de Versões Anteriores do BitDefender

Pode fazer upgrade para o BitDefender Total Security 2011 se estiver a usar a versão beta, 2008, 2009 ou 2010 do BitDefender Total Security 2011.

Há duas formas de fazer o upgrade:

- Instalar o BitDefender Total Security 2011 directamente sobre a antiga versão.Se instalar directamente sobre a versão 2010, as listas de Amigos e Spammers e a Quarentena são automaticamente importadas.
- Remova a anterior versão, reinicie o computador e instale a nova versão tal como descrito na secção “*Instalar BitDefender*” (p. 5).Não serão guardadas as definições do produto.Use este método de upgrade se outros falharem.

5. Remover ou Reparar o BitDefender

Se pretende reparar ou remover o BitDefender Total Security 2011, faça o seguinte a partir do menu Iniciar do Windows: **Iniciar** → **Todos os Programas** → **BitDefender 2011** → **Reparar ou Desinstalar**.

Vai aparecer um assistente para o ajudar a concluir a tarefa desejada.

1. **Reparar ou Remover**

   Seleccione a acção que quer efectuar:

   - **Reparar** - para reinstalar todos os componentes do programa.
   - **Remover** - para remover todos os componetes instalados.

   Nota
   Recomendamos que escolha **Desinstalar** para uma reinstalação limpa.

2. **Confirmar Acção**

   Leia atentamente a informação disponibilizada antes de clicar em **Seguinte** para confirmar a acção.

3. **Progresso**

   Aguarde que o BitDefender conclua a acção que seleccionou.Isto irá demorar vários minutos.

4. **Terminar**

   Os resultados são apresentados.

   Tem de reiniciar o computador para concluir o processo. Clique em **Reiniciar** para reiniciar imediatamente o seu computador ou em **Concluir** para fechar a janela e reiniciar mais tarde.

Introdução

6. Apresentação

Assim que instalar o BitDefender Total Security 2011, o seu computador fica protegido contra todos os tipos de malware (tais como vírus, spyware e cavalos de tróia) e ameaças da Internet (tais como hackers, phishing e spam).

Não é necessário configurar outras definições do BitDefender para além daquelas configuradas durante a instalação.No entanto, poderá querer usufruir das definições do BitDefender para optimizar e melhorar a sua protecção.

De vez em quando, deve abrir o BitDefender e corrigir as incidências existentes.Poderá ter que configurar componentes específicos do BitDefender ou levar a cabo acções preventivas para proteger o seu computador e os seus dados.Se desejar, pode configurar o BitDefender para não o alertar acerca de determinadas incidências.

Se não registou o produto (e não criou uma conta BitDefender), lembre-se de fazer isso antes que o período de testes termine.Tem de criar obrigatoriamente uma conta até 15 dias após instalar o BitDefender (se o registar com uma chave de licença, a data limite aumenta para 30 dias).De outra forma, o BitDefender deixa de ser actualizado.Para mais informaçãoon sobre o processo de registo, por favor consulte o “*Registo e a Minha Conta*” (p. 55).

6.1. A abrir o BitDefender

Para aceder ao interface principal do BitDefender Total Security 2011, utilize o menu Iniciar do Windows, seguindo o caminho **Iniciar** → **Todos os Programas** → **BitDefender 2011** → **BitDefender Total Security 2011** ou, mais rapidamente, faça duplo-clique no ícone do BitDefender que está na área de notificação.

Para mais informações sobre a janela principal da aplicação, por favor consulte “*Janela Principal da Aplicação*” (p. 25).

6.2. Icon da Barra de Tarefas

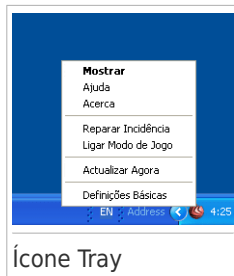
Para gerir todo o produto mais rapidamente, pode usar o ícone da BitDefender que se encontra na barra de tarefas.Se fizer duplo-clique neste ícone, o BitDefender irá abrir. Também clicando com o botão direito do rato sobre ele aparecerá um menu contextual que lhe permitirá uma administração rápida do BitDefender.

Ícone Tray

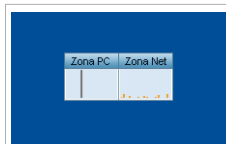
- **Mostrar** - abre o interface principal do BitDefender.
- **Ajuda** - abre o ficheiro de Ajuda, que explica em detalhe como configurar e usar o BitDefender Total Security 2011.
- **Acerca** - abre uma janela onde pode ver informação acerca do BitDefender e onde procurar ajuda caso algo de inesperado lhe apareça.
- **Reparar todos incidências** - ajuda-o a remover as vulnerabilidades de segurança.Se a opção não está disponível, é porque não há incidências a reparar.Para mais informações, por favor consulte "*Reparar Incidência*" (p. 45).
- **Ligar/Desligar Modo de Jogo** - activa / desactiva Modo de Jogo.
- **Actualizar agora** - executa uma actualização imediata.Surge uma nova janela, onde pode ver o estado da actualização.
- **Preferências** - abre uma janela onde pode activar ou desactivas as principais definições do produto e reconfigurar o seu perfil de utilizador.Para mais informação, por favor consulte o "*Configurar Definições Principais*" (p. 48).

O ícone do BitDefender na area de notificação do sistema, informa quando ha incidências a afectar o seu computador ou a forma como o produto funciona, exibindo um símbolo especial, como o que se segue:

Triângulo vermelho com um ponto de exclamação: Questões críticas afectam a segurança do seu sistema. Eles requerem a sua atenção máxima e devem ser corrigidos o mais rapidamente possível.
Letra G:O produto funciona em Modo de Jogo.

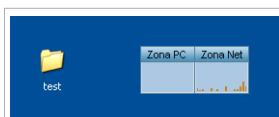
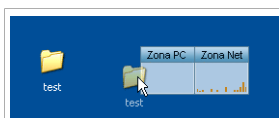
Se o BitDefender não estiver a funcionar, o ícone da area de notificação do sistema fica com a cor cinzenta .Isto normalmente acontece quando a licença de chave expira. Também pode ocorrer quando os serviços da BitDefender não estão a responder ou quando outros erros afectam a actuação normal da BitDefender.

6.3. Barra de Actividade da Análise

A **Barra de Actividade da Análise** é um gráfico de visualização da actividade de verificação no seu sistema.Esta pequena janela, por defeito, está apenas disponível no Modo Avançado.

As barras cinzentas (a **zona PC**) mostram o número de ficheiros analisados por segundo, numa escala de 0 a 50.As barras laranjas apresentadas na **zona Net** mostram o número de Kbytes transferidos (enviados e recebidos da Internet) a cada segundo, numa escala de 0 a 100.

Barra de Actividade da Análise

Nota
A barra de actividade da Análise avisa-o quando a protecção em Tempo-real ou a Firewall está desactivada ao mostrar uma cruz vermelha sobre a área correspondente (**zona PC** ou **zona Net**).

6.3.1. Analisar Ficheiros e Pastas

Pode usar a barra de actividade da análise para analisar rapidamente ficheiros e pastas.Arraste o ficheiro ou a pasta que pretende analisar e deixe-a cair em cima da **Barra de Actividade da Análise**, como apresentado abaixo.

Arraste o ficheiro

Deixe cair o ficheiro

O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise.

Opções de Análise. As opções de análise estão pré-configuradas para obter os melhores resultados de detecção.Se forem detectados ficheiros infectados, o BitDefender irá tentar desinfectá-los (remover o código de malware). Se a desinfecção falha, o assistente de análise antivírus irá permitir-lhe definir outras acções a serem levadas a cabo sobre os ficheiros infectados.As opções de análise são padronizadas e não as pode alterar.

6.3.2. Desactivar/Restaurar Barra de Actividade da Análise

Quando não quiser ver o gráfico de visualização,clique apenas no botão direito e escolha **Esconder**.Para restaurar a barra de actividade da análise, siga os seguintes passos:

1. Abrir o BitDefender.
2. Clique no botão **Opções** no canto superior direito da janela e seleccione **Preferências**.
3. Na categoria Definições Gerais, seleccione a caixa correspondente a **Barra de Actividade da Análise** para a activar.
4. Clique em **OK** para salvar e aplicar as alterações.

6.4. Detecção Automática de Dispositivos

O BitDefender detecta automaticamente quando um dispositivo de armazenamento amovível se liga ao computador, e oferece-se para fazer um scan antes de você aceder aos arquivos.Isto é recomendado para prevenir que virus e malware infectem o seu computador.

Os dispositivos detectados encaixam-se numa destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento USB, tais como pens e discos rígidos externos
- Unidades de Rede Mapeadas (remotas)

Quando dispositivos como estes são detectados, aparece uma janela de alerta.

Para analizar o dispositivo de armazenamento, clique em **Analizar**.O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise.

Se não quiser fazer o scan ao dispositivo, deve clicar **Não**. Nesse caso, uma destas opções podem ser úteis:

- **Não me perguntem novamente acerca deste tipo de dispositivo** - BitDefender não irá mais sugerir que analise dispositivos de armazenagem deste tipo quando eles estiverem ligados ao seu computador.
- **Desactivar detecção automática de dispositivos** - Não será mais solicitado para analisar novos dispositivos de armazenagem quando eles estiverem ligados ao computador.

Se acidentalmente desactivar a detecção automática de dispositivos e pretender activar, ou se deseja configurar as suas definições, siga estes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivirus>Análise Virus**.

3. Na lista de tarefas de análise, localize a tarefa **Análise de Dispositivos**.
4. Clique com o botão direito do rato na tabela e seleccione **Propriedades**.Uma nova janela irá aparecer.
5. Na barra **Visão Geral** e configure as opções de análise como desejar.Para mais informação, por favor consulte o *“Configurar Definições da Análise”* (p. 79).
6. No separador **Detecção**, escolha quais os tipos de dispositivos de armanesamento a ser detectados.
7. Clique em **OK** para salvar e aplicar as alterações.

7. Janela Principal da Aplicação

O BitDefender Total Security 2011 vai de encontro às necessidades quer dos principiantes quer dos utilizadores mais técnicos. Assim, o interface gráfico do utilizador foi desenhado para servir quer uns quer outros.

Pode optar por ver o interface do utilizador em qualquer dos três modos, dependendo do seu computador e sobre a experiência anterior com o BitDefender.

Modo Básico
: Indicado para iniciantes em computadores e pessoas que querem que o BitDefender proteja o seu computador e dados sem incomodos. Este modo é simples de usar e requer a minima interacção da sua parte.

  Tudo o que tem de fazer é reparar as incidências indicadas pelo BitDefender. Um assistente de passo-a-passo intuitivo ajudá-lo-á a resolver essas incidências.Adicionalmente, pode levar a cabo tarefas comuns, tais como actualizar as assinaturas de vírus e os ficheiros do BitDefender ou analisar o computador.

Modo Intermédio
: Destinado a utilizadores com alguns conhecimentos informática, este interface estende o que pode fazer em Modo Básico.

  Pode corrigir problemas separadamente e escolher quais as questões a serem monitorizadas.Além disso, pode gerir remotamente os produtos BitDefender instalados nos computadores de sua casa.

Modo Avançado
: Adequado para os utilizadores com mais conhecimentos tecnicos, este modo permite-lhe configurar completamente cada funcionalidade do BitDefender.Também pode usar todas as tarefas disponiveis para proteger o seu computador e dados.

O modo de visualização é seleccionado durante a instalação.

Para alterar op modo de visualização:

1. Abrir o BitDefender.
2. Clique no botão **Opções** que se encontra no canto superior direito da janela.
3. Seleccione o modo de visualização pretendido no menu.

7.1. Modo Básico

Se é um principiante em informática, o interface do Modo Básico pode ser a escolha mais adequada para si.Este modo é simples de usar e requer a mínima interacção da sua parte.

A janela está organizada em três áreas principais:

Área de Estado
: A informação do estado é apresentada no lado esquerdo da janela.

Área Proteja o seu PC
: Aqui pode tomar as acções necessárias para gerir a sua protecção e manter o seu computador.

Área de Ajuda
: Aqui pode ficar a saber como utilizar o BitDefender Total Security 2011 e obter ajuda.

O botão **Opções** no canto superior direito da janela permite-lhe alterar o modo do interface e configurar as definições principais do programa.

No canto inferior direito da janela, pode encontrar vários links úteis.

Link	Descrição
Informação da Licença	Abre uma janela onde pode ver a informação da chave de licença actual e registar o seu produto com a nova chave de licença.
Histórico	Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema.
Ajuda e Suporte	Clique nesta hiperligação se precisar de ajuda com o BitDefender.
?	Dá-lhe acesso ao ficheiro de ajuda que lhe mostra como usar o BitDefender.

7.1.1. Estado da Área

A informação do estado é apresentada no lado esquerdo da janela.

- **Estado** - Alerta-o se incidências afectarem o seu computador e ajuda-o a repará-las.Ao clicar em **Reparar Incidências**, o assistente irá ajuda-lo a remover facilmente quaisquer ameaça do seu computador e segurança de dados.Para mais informações, por favor consulte “*Reparar Incidência*” (p. 45).
- **Estado da Licença** mostra quantos dias faltam até à licença expirar.Se estiver a utilizar uma versão de avaliação lou se a sua licença estiver a expirar, pode clicar em **Comprar Agora** para adquirir uma chave de licença.Para mais informações, por favor consulte “*Registo e a Minha Conta*” (p. 55).

7.1.2. Área Proteja o seu PC

Aqui pode tomar as acções necessárias para gerir a sua protecção e manter o seu computador.

Estão disponíveis três botões:

- **Segurança** disponibiliza os atalhos para as tarefas e definições de segurança.
- **Optimizar** permite-lhe efectuar tarefas que melhoram o desempenho e a resposta do seu computador.
- **Meus Instrumentos** permite-lhe criar atalhos para as suas tarefas e definições favoritas.

Para efectuar uma tarefa ou configurar definições, clique no respectivo botão e escolha o instrumento pretendido no menu.Para adicionar ou remover atalhos, clique no respectivo botão e escolha **Mais Opções**.Para mais informações, por favor consulte “*Ferramentas*” (p. 36).

7.1.3. Área de Ajuda

Aqui pode ficar a saber como utilizar o BitDefender Total Security 2011 e obter ajuda.

Dicas Inteligentes são uma forma fácil e divertida de aprender as melhores práticas para proteger o seu PC e como utilizar o BitDefender Total Security 2011.

Se precisar de ajuda, escreva uma palavra-chave ou uma pergunta no campo **Ajuda e Suporte** e clique em **Procurar**.

7.2. Modo Intermédio

Destinado a utilizadores com conhecimentos médios de informática, o Modo Intermédio é um interface simples que lhe dá acesso a todos os módulos num nível básico. Terá de acompanhar as advertências e alertas críticos e corrigir problemas indesejáveis.

A janela do Modo Intermédio está organizada em vários separadores.

Painel
: O painel ajuda-o a monitorizar e gerir facilmente a sua protecção.

Segurança
: Mostra o estado das definições de segurança e ajuda a corrigir os problemas detectados.Pode executar tarefas de segurança ou configurar definições de segurança.

TUNE-UP
: Mostra o estado das opções do BitDefender desenhadas para melhorar o desempenho do seu sistema juntamente com os links das tarefas de tuneup.

Gestor de Ficheiros
: Mostra o estado do cofre de ficheiros e dos módulos de backup juntamente com os links para os cofres de ficheiros e das tarefas de backup.

REDE
: Mosta a estrutura da rede pessoal BitDefender.Aqui é onde pode levar a cabo diversas acção para configurar os produtos BitDefender instalados na sua rede pessoal.Desta forma, pode gerir a segurança da sua rede pessoal, a partir de um só computador.

O botão **Opções** no canto superior direito da janela permite-lhe alterar o modo do interface e configurar as definições principais do programa.

No canto inferior direito da janela, pode encontrar vários links úteis.

Link	Descrição
Informação da Licença	Abre uma janela onde pode ver a informação da chave de licença actual e registar o seu produto com a nova chave de licença.
Histórico	Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema.
Comprar/Renovar	Ajuda-o a adquirir uma chave de licença para o seu produto BitDefender Total Security 2011.
Ajuda e Suporte	Clique nesta hiperligação se precisar de ajuda com o BitDefender.
?	Dá-lhe acesso ao ficheiro de ajuda que lhe mostra como usar o BitDefender.

7.2.1. Painel

O painel ajuda-o a monitorizar e gerir facilmente a sua protecção.

O painel é composto de várias secções:

- **Detalhes do Estado** indica o estado de cada módulo principal usando frases explícitas e um dos seguintes ícones:

  Círculo verde com uma marca de verificação: Nenhuma incidências a afectar o estado de segurança.O seu computador e os seus dados estão protegidos.

  Circulo vermelho com um ponto de exclamação: Há incidências a afectarem a segurança do seu sistema.Incidências criticas requerem a sua atenção imediata. Incidências que não sejam críticas também deverão ser abordadas com a maior brevidade possível

  Círculo azul com letra i: Uma ou várias tarefas devem de ser levadas a cabo de forma a optimizar o sistema ou proteger os seus dados.

Círculo cinzento com um ponto de exclamação: A actividade dos componentes deste módulo não estão a ser monotorizados. Assim, não há informação disponível sobre o estado de segurança.Não há incidências específicas relativamente a este módulo.

Clique no nome de um módulo para ver mais detalhes acerca do seu estado e para configurar o estado da monitorização dos seus componentes.

- **Estado da Licença** mostra quantos dias faltam até à licença expirar.Se estiver a utilizar uma versão de avaliação lou se a sua licença estiver a expirar, pode clicar em **Comprar Agora** para adquirir uma chave de licença.Para mais informações, por favor consulte “*Registo e a Minha Conta*” (p. 55).
- **Meus Instrumentos** permite-lhe criar atalhos para as suas tarefas e definições favoritas.Para mais informações, por favor consulte “*Ferramentas*” (p. 36).
- **Dicas Inteligentes** são uma forma fácil e divertida de aprender as melhores práticas para proteger o seu PC e como utilizar o BitDefender Total Security 2011.

7.2.2. Segurança

O separador Segurança permite-lhe gerir a segurança do seu computador e dos seus dados .

“Estado da Área” (p. 29)
“Tarefas Rápidas” (p. 30)

Estado da Área

A área de estado é onde pode ver a lista completa de componentes de segurança monotorizados e o seu estado actual.Ao monotorizar cada módulo de segurança, o BitDefender irá informá-lo não só quando configurar definições que possam afectar a segurança do seu computador, mas também quando se esqueceu de realizar tarefas importantes.

O estado actual de um componente é indicado utilizando frases exclarecedoras e um dos seguintes ícones:

Círculo verde com uma marca de verificação: Não há incidências a infectarem o componente.

Circulo vermelho com um ponto de exclamação: Há incidências a infectarem o componente.

Apenas clique no botão **Corrigir** correspondendo à frase para corrigir a incidência reportada.Se uma das incidências não for reparada no momento, siga o assistente para a reparar.

Para configurar os instrumentos a monitorizar:

1. Clique em **Adicionar/Editar Lista**.

2. Para activar ou desactivar a monitorização de um determinado item, utilize o respectivo botão.
3. Clique em **Fechar** para guardar as alterações e fechar a janela.

Importante

Para se certificar de que o seu sistema está completamente protegido, por favor permita a análise a todos os componentes e resolva todas as incidências reportadas.

Tarefas Rápidas

Aqui pode encontrar links para as mais importantes tarefas de segurança:

- **Actualizar agora** - executa uma actualização imediata.
- **Análise Minuciosa ao Sistema** - inicia uma análise completa do seu computador (excepto arquivos). Para tarefas de análise a pedido adicionais clique na seta neste botão e seleccione uma tarefa de análise diferente.
- **Análise Personalizada** - abre um assistente que lhe permite criar e utilizar uma tarefa de análise personalizada.
- **Análise de Vulnerabilidade** - inicia um assistente que verifica o seu sistema em busca de vulnerabilidades e ajuda-o a repará-las.
- **Controlo Parental** - abre a janela de configuração do Controlo Parental.Para mais informação, por favor consulte o "*Controlo Parental* " (p. 106).
- **Configurar Firewall** - abre uma janela onde pode visualizar e configurar as definições da Firewall.Para mais informação, por favor consulte o "*Firewall*" (p. 132).

7.2.3. TUNE-UP

BitDefender vem com um módulo de Optimização que o ajuda a manter a integridade do seu sistema. As ferramentas de manutenção oferecidas são criticas para o melhoramento do desempenho do seu sistema e para uma gestão eficiente do espaço do seu disco duro.

"Estado da Área" (p. 30)
"Tarefas Rápidas" (p. 31)

Estado da Área

O estado actual de um componente é indicado utilizando frases exclarecedoras e um dos seguintes ícones:

Círculo verde com uma marca de verificação: Não há incidências a infectarem o componente.
Círculo azul com letra i: É recomendável que leve a cabo a tarefa.

Para levar a cabo uma tarefa recomendada, clique no botão correspondente **Executar Agora** e siga o assistente.Para mais informação, por favor consulte o *“TUNE-UP”* (p. 185).

Importante

Para melhorar o desempenho do seu computador, é recomendado que execute todas as tarefas periodicamente.

Para configurar os instrumentos de optimização a monitorizar:

1. Clique em **Adicionar/Editar Lista**.
2. Para activar ou desactivar a monitorização de um determinado item, utilize o respectivo botão.
3. Clique em **Fechar** para guardar as alterações e fechar a janela.

Tarefas Rápidas

É aqui que pode encontrar o caminho para as tarefas do Tuneup:

- Desfragmentador reorganiza os dados no disco rígido de forma a que as partes constituintes de cada ficheiro sejam armazenadas juntas e de forma contínua.
- Limpeza do PC remove os ficheiros temporários da Internet e as cookies, os ficheiros não utilizados do sistema e os atalhos recentes dos documentos.
- O Localizador de Duplicados encontra e apaga ficheiros que se encontram duplicados no seu sistema.
- Limpar Registo identifica e apaga referências orfãs ou inválidas do Registo do Windows.De forma a manter o Registo do Windows limpo e optimizado, é recomendável que execute o seu Limpa Registo uma vez por mês.
- O Restaurar Registo pode recuperar as chaves de registo previamente apagadas do Registo do Windows no uso do Limpa Registo BitDefender.
- Destruidor Ficheiros apaga permanentemente os ficheiros e os seus vestígios do sistema.
- Optimizador de Desempenho ajuda a identificar e encerrar as aplicações que estão a abrandar o seu computador para melhorar o desempenho do seu sistema.

7.2.4. Gestor de Ficheiros

No separador Armazenamento de Ficheiros, pode proteger proactivamente os seus dados fazendo cópias de segurança dos ficheiros mais importantes. Também pode guardar os seus ficheiros sensíveis em cofres de ficheiros encriptados para impedir que sejam acedidos por outras pessoas.

“Estado da Área” (p. 32)
“Tarefas Rápidas” (p. 32)

Estado da Área

O estado actual de um componente é indicado utilizando frases exclarecedoras e um dos seguintes ícones:

Círculo verde com uma marca de verificação: Não há incidências a infectarem o componente.

Circulo vermelho com um ponto de exclamação: Há incidências a infectarem o componente.

Círculo azul com letra i: É recomendável que leve a cabo a tarefa.

Apenas clique no botão **Corrigir** correspondendo à frase para corrigir a incidência reportada.

Para levar a cabo uma tarefa recomendada, clique no botão correspondente **Executar Agora** e siga o assistente.Para mais informação, por favor consulte o "*Backup*" (p. 148).

Para configurar os instrumentos a monitorizar:

1. Clique em **Adicionar/Editar Lista**.
2. Para activar ou desactivar a monitorização de um determinado item, utilize o respectivo botão.
3. Clique em **Fechar** para guardar as alterações e fechar a janela.

Tarefas Rápidas

Estão disponíveis os seguintes botões:

- **Backup Local** - ajuda a fazer cópias de segurança dos seus dados mais valiosos no seu computador, num CD, num local de rede ou em qualquer outra unidade física e restaurá-los, se necessário.Clique no botão e selecione a função desejada no menu.O assistente acompanha-o no desempenho desta tarefa.
- **Adicionar ao Cofre** - inicia o assistente que lhe permite armazenar de forma privada os seus ficheiros / documentos importantes ao encriptá-los em drives de cofre especiais.
- **Remover do Cofre** - inicia o assistente que lhe permite apagar dados do cofre de ficheiros.
- **Ver cofre** - inicia o assistente que lhe permite ver o conteúdo do cofre de ficheiros.
- **Fechar cofre** - inicia o assistente que lhe permite fechar o cofre de forma a dar início à protecção do seu conteúdo.

Para mais informações sobre como fazer cópias de segurança e restaurar dados, por favor consulte "*Backup*" (p. 148).Para mais informações sobre como proteger os seus ficheiros com cofres de ficheiros, consulte "*Encriptação Ficheiro*" (p. 174).

7.2.5. REDE

Aqui é onde pode levar a cabo diversas acção para configurar os produtos BitDefender instalados na sua rede pessoal.Desta forma, pode gerir a segurança da sua rede pessoal, a partir de um só computador.

Para mais informações, por favor consulte "*A Sua Rede*" (p. 199).

7.3. Modo Avançado

O Modo Avançado dá-lhe acesso a cada componente específico do BitDefender. Aqui é onde pode configurar o BitDefender em detalhe.

Nota

O Modo Avançado é adequado para os utilizadores que têm conhecimentos informáticos acima da média, que conhecem o tipo de ameaças a que um computador está exposto e como funcionam os programas de segurança.

Do lado esquerdo da janela existe um menu que contém todos os módulos de segurança.Cada módulo possui um ou mais separadores onde pode configurar as respectivas definições de segurança ou executar tarefas de segurança e de administração.A lista seguinte descreve resumidamente cada módulo.Para mais informações, por favor consulte "Configuração e Gestão" (p. 59).

Geral
: Permite-lhe aceder às definições gerais ou ver o painel e a info detalhada do sistema.

Antivírus
: Permite-lhe configurar o escudo de vírus e as operações de análise em detalhe, definir excepções e configurar o módulo de quarentena.Aqui pode configurar a protecção antiphishing e o Consultor de Procura.

Antispam
: Permite-lhe manter a pasta A Receber livre de SPAM e também configurar as definições do antispam em detalhe.

Controlo Parental
: Permite-lhe proteger as suas crianças contra o conteúdo inapropriado, ao usar as suas regras personalizadas de acesso ao computador.

Controlo de Privacidade
: Permite-lhe evitar que sejam roubados dados do seu computador e protege a sua privacidade enquanto se encontra on-line.

Firewall
: Permite-lhe proteger o seu computador de tentativas de ligações internas e externas não-autorizadas. É bastante semelhante a um guarda que está à sua

porta – irá manter um olhar atento na sua ligação à Internet e rastrear a quem permitir e a quem bloquear o acesso à mesma.

Vulnerabilidade
: Permite-lhe manter o software crucial para o seu PC sempre actualizado.

Backup
: Permite-lhe fazer backup dos seus dados no seu computador, numa drive amovível ou num local de rede para assegurar que os pode restaurar quando necessário.

Encriptação
: Permite-lhe encriptar as comunicações do Yahoo e Windows Live (MSN) Messenger e também encriptar localmente os seus ficheiros critícos, as suas pastas ou partições.

TuneUp
: Permite-lhe melhorar o desempenho do seu computador ao desfragmentar o seu disco, limpar o registo e os ficheiros duplicados, etc.

Modo Jogo/Portátil
: Permite-lhe adiar as tarefas agendadas BitDefender enquanto o seu portátil está a funcionar a bateria e também elimina alertas e pop-ups enquanto está a jogar.

A Sua Rede
: Permite-lhe configurar e gerir vários computadores do seu lar.

Actualização
: Permite-lhe obter info das últimas actualizações, actualizar o produto e configurar o processo de actualização em detalhe.

Registo
: Permite-lhe registar o BitDefender Total Security 2011, mudar a chave de licença ou criar uma conta BitDefender.

O botão **Opções** no canto superior direito da janela permite-lhe alterar o modo do interface e configurar as definições principais do programa.

No canto inferior direito da janela, pode encontrar vários links úteis.

Link	Descrição
Informação da Licença	Abre uma janela onde pode ver a informação da chave de licença actual e registar o seu produto com a nova chave de licença.
Histórico	Permite-lhe ver um histórico detalhado de todas as tarefas levadas a cabo pelo BitDefender no seu sistema.

Link	Descrição
Comprar/Renovar	Ajuda-o a adquirir uma chave de licença para o seu produto BitDefender Total Security 2011.
Ajuda e Suporte	Clique nesta hiperligação se precisar de ajuda com o BitDefender.
?	Dá-lhe acesso ao ficheiro de ajuda que lhe mostra como usar o BitDefender.

8. Ferramentas

No Modo Básico ou no modo Intermédio do BitDefender, pode personalizar o seu painel de instrumentos adicionado atalhos paras as tarefas e definições que são mais importantes para si.Desta forma, pode aceder rapidamente às funcionalidades que utiliza normalmente e às definições avançadas sem ter de mudar para um modo de utilizador mais avançado.

Consoante o modo do interface de utilizador, os atalhos adicionados aos Meus Instrumentos estão disponíveis da seguinte forma:

Modo Básico
: Na área Proteja o seu PC, clique em Meus Instrumentos.Irá aparecer um menu.Clique num atalho para executar o respectivo instrumento.

Modo Intermédio
: Os atalhos aparecem em Meus Instrumentos.Clique num atalho para executar o respectivo instrumento.

Para abrir a janela onde pode seleccionar os atalhos que irão aparecer nos Meus Instrumentos, proceda da seguinte forma:

Modo Básico
: Na área Proteja o Seu PC, clique em Meus Instrumentos e escolha **Mais Opções**.

Modo Intermédio
: Clique num dos botões em Meus Instrumentos ou na hiperligação **Configurar Meus Instrumentos**.

Utilize os botões para seleccionar os recursos a adicionar aos Meus Instrumentos.Pode seleccionar uma das seguintes categorias de instrumentos.

- **Tarefas de Análise**

  Adicione as tarefas que utiliza regularmente para analisar se há ameaças de segurança no seu sistema.

Tarefa de Análise	Descrição
Análise Minuciosa	Analisa todo o sistema.Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.
Análise Completa	Analisa todo o sistema, excepto arquivos.Na configuração por defeito, analisa todos os tipos de malware excepto rootkits.
Análise Rápida	A Análise Rápida utiliza a análise nas nuvens para detectar malware em execução no seu

Tarefa de Análise	Descrição
	sistema.Normalmente, a realização de uma Análise Rápida demora menos de um minuto e utiliza uma facção dos recursos do sistema necessários para uma análise de vírus normal.
Análise Personalizada	Inicia um assistente que lhe permite criar uma tarefa de análise personalizada.
Analisar Os Meus Documentos	Use esta tarefa para analisar pastas de utilizadores actuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de trabalho segura e aplicações limpas a serem executadas no arranque.
Agendar as Minhas Análises	Encaminha para a janela de definições do Antivírus, onde pode personalizar as tarefas de análise a pedido.

Para mais informações sobre as tarefas de análise, consulte *"Gerir Tarefas de Análise Existentes"* (p. 76).

- **Tarefas de Optimização**

Adicione as tarefas que utiliza normalmente para melhorar a velocidade do seu sistema.

Tarefa de Optimização	Descrição
Localizador de Duplicados	Encontra e apaga ficheiros que se encontram duplicados no seu sistema.
Limpa Registo	Identifica e elimina referências inválidas ou desactualizadas no Registo do Windows.
Limpeza do PC	Remove os ficheiros temporários da Internet e as cookies, os ficheiros não utilizados do sistema e os atalhos recentes dos documentos.

Para mais informações sobre as tarefas de optimização, consulte *"TUNE-UP"* (p. 185).

- **Tarefas de Backup**

Adicione as tarefas que utiliza regularmente para fazer cópia de segurança dos seus dados.

Tarefa de Backup	Descrição
Backup Local	Faça um backup local dos seus dados.
Restauro Local	Restaurar dados de um Backup Local

Para mais informações sobre as tarefas de backup, consulte “*Backup*” (p. 148).

- **Definições**

  Adicione atalhos para as definições do BitDefender que pretende configurar:

Definições	Descrição
Definições do Antivírus	Configure o módulo do Antivírus. Para mais informações, consulte “*Protecção Antivírus*” (p. 64).
Configurar Firewall	Configure o módulo da Firewall. Para mais informações, consulte “*Firewall*” (p. 132).
Controlo Parental	Configure o módulo do Controlo Parental. Para mais informações, consulte “*Controlo Parental* ” (p. 106).
Modo de Jogo	Active o Modo Jogo. Para mais informações, por favor consulte “*Modo de Jogo*” (p. 193).
Modo Portátil	Active o Modo Portátil. Para mais informações, por favor consulte “*Modo Portátil*” (p. 196).
Actualizar Agora	Active uma actualização do BitDefender. Para mais informações, por favor consulte “*Actualização*” (p. 203).
Ver & Corrigir Todas as Incidências	Abra um assistente que o irá ajudar a corrigir todas as incidências de segurança que estão a afectar o seu sistema. Para mais informações, por favor consulte “*Reparar Incidência*” (p. 45).

- **Ajuda & Suporte**

  Entre na secção de suporte. Para mais informações, por favor consulte “Contacte-nos Directamente Do Seu Produto BitDefender” (p. 255).

9. Alertas e Pop-ups

BitDefender utiliza pop-ups e alertas para informar sobre o funcionamento ou sobre eventos especiais que poderão interessar-lhe e perguntar o que fazer sempre que necessário.Este capítulo apresenta os pop-ups e alertas do BitDefender que poderão surgir.

Pop-ups são pequenas janelas que aparecem temporariamente no ecrã a informar sobre vários eventos do BitDefender, como análise do correio electrónico, um novo computador que iniciou sessão na rede sem fios, uma nova regra de firewall, etc.Quando aparecerem pop-ups, ser-lhe-á pedido que clique no botão **OK** ou numa hiperligação, nada mais.

Os alertas são janelas a pedir que indique uma acção ou a informar sobre algo muito importante (por exemplo, a detecção de um vírus).Para além das janelas de alerta, poderá receber mensagens electrónicas ou instantâneas ou alertas na página de Internet.

Os pop-ups e alertas BitDefender incluem:

- Alertas Antivírus
- Alertas do Controlo Activo de Vírus
- Alertas de Detecção de Dispositivo
- Pop-ups e Alertas da Firewall
- Páginas de Alerta Antiphishing
- Mensagens de Alerta do Controlo Parental
- Alertas do Controlo de Privacidade

9.1. Alertas Antivírus

BitDefender protege-o contra vários tipos de malware, como vírus, spyware ou rootkits.Ao detectar um vírus ou outro malware, o BitDefender aplica uma determinada acção sobre o ficheiro infectado e informa-o através de uma janela de alerta.

Pode ver o nome do vírus, o caminho para o ficheiro infectado e a acção aplicada pelo BitDefender.

Clique **OK** para fechar a janela.

Importante

Quando é detectado um vírus, a melhor opção é analisar a totalidade do sistema para garantir que não há mais vírus.Para mais informação, por favor consulte o "*Como Posso Analisar Ficheiros e Pastas?*" (p. 208).
Se o vírus não tiver sido bloqueado, por favor consulte "*Remover Malware do Sistema*" (p. 244).

9.2. Alertas do Controlo Activo de Vírus

O Controlo Activo de Vírus pode ser configurado para o alertar e pedir-lhe para agir sempre que uma aplicação tentar executar umas acção possivelmente maliciosa.

Se estiver a utilizar o Modo Básico ou o Modo Intermédio, um pop-up irá aparecer sempre que o Controlo de Vírus Activo bloquear uma aplicação potencialmente prejudicial.Se estiver a utilizar o Modo Avançado, ser-lhe-á pedida uma acção, através de uma janela de alerta, sempre que que uma aplicação apresentar um comportamento malicioso.

Se conhece e confia na aplicação detectada, clique em **Permitir**.

Se deseja fechar imediatamente a aplicação, clique em **OK**.

Seleccione a caixa de selecção **Lembrar esta acção para esta aplicação** antes de fazer a sua escolha e o BitDefender tomará a mesma acção no futuro para a aplicação detectada.A regra que é então criada será listada na janela da configuração do Controlo Activo de Vírus.

9.3. Alertas de Detecção de Dispositivo

O BitDefender detecta automaticamente quando um dispositivo de armazenamento amovível se liga ao computador, e oferece-se para fazer um scan antes de você aceder aos arquivos.Isto é recomendado para prevenir que virus e malware infectem o seu computador.

Os dispositivos detectados encaixam-se numa destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento USB, tais como pens e discos rígidos externos
- Unidades de Rede Mapeadas (remotas)

Quando dispositivos como estes são detectados, aparece uma janela de alerta.

Para analizar o dispositivo de armazenamento, clique em **Analizar**.O assistente do Scan de Antivirus irá aparecer e guiá-lo durante o processo.

Se não quiser fazer o scan ao dispositivo, deve clicar **Não**. Nesse caso, uma destas opções podem ser úteis:

- **Não me perguntem novamente acerca deste tipo de dispositivo** - BitDefender não irá mais sugerir que analise dispositivos de armazenagem deste tipo quando eles estiverem ligados ao seu computador.
- **Desactivar detecção automática de dispositivos** - Não será mais solicitado para analisar novos dispositivos de armazenagem quando eles estiverem ligados ao computador.

Se acidentalmente desactivar a detecção automática de dispositivos e pretender activar, ou se deseja configurar as suas definições, siga estes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivirus>Análise Virus**.
3. Na lista de tarefas de análise, localize a tarefa **Análise de Dispositivos**.
4. Clique com o botão direito do rato na tabela e seleccione **Propriedades**.Uma nova janela irá aparecer.
5. Na barra **Visão Geral** e configure as opções de análise como desejar.Para mais informação, por favor consulte o *"Configurar Definições da Análise"* (p. 79).
6. No separador **Detecção**, escolha quais os tipos de dispositivos de armanesamento a ser detectados.
7. Clique em **OK** para salvar e aplicar as alterações.

9.4. Pop-ups e Alertas da Firewall

A firewall utiliza pop-ups para informar sobre os vários eventos relacionados com a sua ligação de rede (por exemplo, quando um novo computador liga à sua rede sem fios, quando uma aplicação é autorizada a aceder à Internet ou quando é bloqueada uma análise de porta).Estes pop-ups poderão ser úteis para detectar tentativas de intrusão e proteger a sua rede contra ameaças.

Se estiver a utilizar o Modo Avançado, ser-lhe-á pedida uma acção, através de uma janela de alerta, sempre que que uma aplicação desconhecida tentar ligar à Internet.

Pode ver o seguinte: a aplicação que se está a tentar ligar à internet, o caminho do ficheiro da aplicação, o destino, o protocolo usado e a porta na qual a aplicação se está a tentar ligar.

Clique **Permitir** para permitir o tráfego (entrada e saída) gerado por esta aplicação a partir do local host para qualquer destino, no respectivo protocolo IP protocol e em todas as portas. Se clicar em **Bloquear**, será negado completamente o acesso à Internet por parte da aplicação no respectivo protocolo IP.

Importante

Permitir tentativas de ligação de entrada apenas de IP's ou domínios em que confia totalmente.

Baseado na sua resposta, uma regra será criada, aplicada e listada na tabela. A próxima vez que a aplicação se tentar ligar, esta regra será aplicada por defeito.

Se estiver no Modo Básico ou no Modo Intermédio, a tentativa de ligação será automaticamente bloqueada.

9.5. Alertas Antiphishing

Com a protecção antiphishing activada, o BitDefender alerta quando tentar aceder a páginas da Internet que poderão roubar informações pessoais.Antes de poder aceder a uma página de Internet desse tipo, o BitDefender vai bloquear essa página e mostra um alerta genérico.

Verifique o endereço da página de Internet na barra de endereços do seu navegador.Procure pistas que poderão indicar que a página de Internet é utilizada para roubar a identidade.Se o endereço da página for suspeito, é recomendado que não o abra.

Aqui estão algumas dicas que poderá achar úteis:

- Se escreveu o endereço de um sítio de Internet legítimo, verifique se o endereço está correcto. Se estiver incorrecto, torne a escrever e navegue novamente para a página.
- Se clicar numa hiperligação de uma mensagem electrónica ou instantânea, verifique quem a enviou. Se o remetente for desconhecido, é provável que seja uma tentativa de phishing. Se conhecer o remetente, deve confirmar se essa pessoa enviou realmente a hiperligação.
- Se chegou à página ao navegar na Internet, consulte a página onde encontrou a hiperligação (clique no botão Retroceder do seu navegador).

Se quiser visualizar a página de Internet, clique na hiperligação correspondente para aplicar uma das seguintes acções:

- **Visualizar a página de Internet apenas desta vez.** Não há qualquer risco desde que não submeta informações na página de Internet.Se a página de Internet for legítima, pode adicioná-la à Lista Branca (clique na barra de ferramentas Antiphishing BitDefender e seleccione **Adicionar à Lista Branca**).
- **Adicionar a página de Internet à Lista Branca.** A página de Internet será apresentada imediatamente e o BitDefender não tornará a alertar sobre ela.

Importante

Adicione à Lista Branca apenas as páginas de Internet em que confia plenamente (por exemplo, o sítio do seu banco, lojas em linha conhecidas, etc.).O BitDefender não verifica a existência de phishing nas páginas de Internet da Lista Branca.

Pode gerir a protecção antiphishing e a Lista Branca com a barra de ferramentas do BitDefender no seu navegador de Internet.Para mais informação, por favor consulte o *“Gerir a Protecção Antiphishing do BitDefender no Internet Explorer e Firefox”* (p. 89).

9.6. Mensagens de Alerta do Controlo Parental

Pode configurar o Controlo Parental para bloquear:

- Páginas web inapropriadas.
- ligação à Internet, durante determinados períodos de tempo (tal como o período de estudo).
- páginas web, mensagens de e-mail e mensagens instântaneas que contenham determinadas palavras-chave.
- aplicações tais como: jogos, programas de partilha de ficheiros e outros.
- mensagens instântaneas enviadas por contacto IM para além dos que estão permitidos.

O utilizador é informado sempre que uma actividade é bloqueada através de uma mensagem de alerta específica (por exemplo, uma página de Internet, mensagem electrónica ou mensagem instantânea com um alerta padrão).São fornecidas informações detalhadas para que o utilizador possa saber porque é que a actividade foi bloqueada.

9.7. Alertas do Controlo de Privacidade

O Controlo de Privacidade oferece aos utilizadores mais experientes alguns recursos adicionais para proteger a identidade.Será consultado sobre as acções a aplicar através de janelas de alerta específicas se escolher activar um dos seguintes componentes:

- O Controlo do Registo - irá pedir a sua permissão sempre que um programa tentar modificar uma entrada de registo de forma a poder ser executado durante o arranque do Windows.

- O Controlo de Cookies - irá pedir a sua permissão sempre que um novo site web tentar definir uma cookie.

- O Controlo de script - irá pedir a sua permissão sempre que um site web tente activar um script ou outro conteúdo activo.

9.7.1. Alertas de Registo

Se activar o Controlo de Registo, ser-lhe-á pedida permissão sempre que um programa tentar modificar uma entrada de registo de forma a poder ser executado durante o arranque do Windows.

Poderá ver o programa que está a tentar alterar o registo do Windows.

Nota
O BitDefender irá, normalmente, alertá-lo quando instalar novos programas que necessitem decorrer na próxima inicialização do seu computador. Na maioria dos casos, estes programas são legítimos e podem ser confiáveis.

Se não reconhece o programa e lhe parecer suspeito, clique em **Bloquear** para evitar que ele modifique o registo do Windows.De outra forma, clique em **Permitir** para permitir a modificação.

Baseado na sua resposta, a regra é criada e listada na tabela de regras.A mesma acção será aplicada sempre que este programa tentar modificar uma entrada no registo.

Para mais informação, por favor consulte o “*Controlo de registo*” (p. 128).

9.7.2. Alertas de Script

Se activar o Controlo de Scripts, ser-lhe-á pedida autorização sempre que um novo sítio de Internet tentar executar um script ou outro conteúdo activo.

Pode ver o nome do recurso.

clique em **Sim** ou **Não** e será criada, aplicada e listada uma regra na tabela das regras.A mesma acção será aplicada automaticamente sempre que o respectivo sítio de Internet tentar executar o conteúdo activo.

Nota
Algumas páginas de Internet poderão não ser correctamente visualizadas se bloquear o conteúdo activo.

Para mais informação, por favor consulte o “*Controlo de script* ” (p. 130).

9.7.3. Alertas de Cookie

Quando activado, o Controlo de Cookies vai pedir-lhe autorização sempre que um novo sítio de Internet tenta definir ou pedir um cookie.

Pode ver o nome da aplicação que está a tentar enviar um ficheiro de cookie.

clique em **Sim** ou **Não** e será criada, aplicada e listada uma regra na tabela das regras.A mesma acção será automaticamente aplicada sempre que efectuar a ligação ao respectivo sítio.

Para mais informação, por favor consulte o “*Controlo de cookies* ” (p. 129).

10. Reparar Incidência

O BitDefender utiliza um sistema de emissão de monitoramento para detectar e informá-lo sobre os problemas que podem afectar a segurança do seu computador e dos seus dados. Por defeito, ele irá acompanhar apenas algumas questões que são consideradas muito importantes. No entanto, pode sempre configurá-lo conforme necessário, escolhendo as questões específicas sobre que deseja ser notificado.

É assim que as questões pendentes são notificadas:

- É mostrado um símbolo especial sobre o ícone do BitDefender no tabuleiro de sistema a indicar incidências pendentes.Além disso, se mover o cursor do rato sobre o ícone, uma janela pop-up irá confirmar a existência de questões pendentes.
- Quando abre o BitDefender, a área de Estado da Segurança vai indicar o número de incidências que afectam o seu sistema.
  - No Modo Básico, o estado de segurança é apresentado no lado esquerdo da janela.
  - No Modo Avançado, vá a **Geral > Painel** para verificar o estado da segurança.

10.1. Assistente Reparar Incidências

A forma mais fácil de corrigir as incidências existentes é seguir o passo-a-passo o **assistente Reparar Incidências** .Para abrir o assistente, faça uma das seguintes coisas:

- Clique com o botão direito do rato no ícone do BitDefender na area de notificação e seleccione **Reparar Incidências**.
- Abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:
  - No Modo Básico, clique em **Ver Todas as Incidências**.
  - No Modo Avançado, vá a **Geral > Painel** e clique em **Ver Todas as Incidências**.

Nota
Também pode adicionar um atalho a Meus Instrumentos.

É apresentada uma lista das ameaças de segurança existentes no seu computador.

Todas as incidências estão seleccionadas para serem solucionadas. No caso de existir uma incidência que não quer resolver, escolha a caixa de selecção correspondente. Se o fizer, o estado mudará para **Saltar**.

Nota
Se não pretender ser notificado sobre determinadas incidências, tem de configurar o sistema de alerta, tal como descrito na secção seguinte.

Para resolver a incidência seleccionada, clique em **Iniciar**. Algumas incidências são tratadas imediatamente. Para outras, o assistente ajuda-o a resolvê-las.

A incidência que este assistente o ajuda a tratar pode ser agrupada numa destas categorias:

- **Desactivar definições de segurança.** Tais incidências são reparadas imediatamente, ao activar as respectivas definições de segurança.
- **Ferramentas preventivas de segurança que deve realizar.** Um exemplo dessa tarefa é a análise ao seu computador. É recomendado que faça uma análise ao seu computador pelo menos uma vez por semana. O BitDefender irá automaticamente fazê-lo por si na maioria dos casos. Contudo, se alterou o agendamento das análises ou se o agendamento não se completou, será notificado sobre essa incidência.

  Quando reparar a incidência, o assistente ajuda-o a completar com sucesso a tarefa.
- **Vulnerabilidades dos Sistema.** O BitDefender verifica automaticamente o seu sistema por vulnerabilidades e alerta-o sobre eles.As vulnerabilidades do sistema incluem:
  - Senhas fracas para as contas de utilizador do Windows.
  - Software desactualizado no seu computador
  - actualizações do Windows em falta.
  - As actualizações automáticas do Windows estão desativadas.

  Quando essas incidências estão a ser reparadas, o assistente de análise de vulnerabilidades é iniciado. Este assistente ajuda-o a reparar as vulnerabilidades de sistema detectadas.Para mais informação, por favor consulte o “*A analisar em busca de Vulnerabilidades*” (p. 145).

10.2. Configurar os Alertas de Estado

O sistema de alerta de estado é pré-configurado para monitorizar e alertar sobre as incidências mais importantes que poderão afectar a segurança do seu computador e dos seus dados.Para além das incidências monitoradas por defeito, existem outras incidências de que pode vir a ser informado.

Pode configurar o sistema de alerta para melhor responder às suas necessidades de segurança escolhendo as incidências específicas sobre as quais pretende receber informações.Pode fazer isto no Modo Intermédio ou no Modo Avançado.

- No Modo Intermédio, a o sistema de alerta pode ser configurado a partir de locais diferentes.Siga estes passos:
  1. Vá até **Segurança**, **Tuneup** ou ao separador **Armazenamento de Ficheiros**.
  2. Clique na hiperligação **Adicionar/Editar Lista** na área de Estado.
  3. Utilize o botão do item para alterar o respectivo estado de alerta.
- No Modo Avançado, o sistema de alerta pode ser configurado a partir de um local central.Siga estes passos:
  1. Vá a **Geral > Painel**.
  2. Clique em **Adicionar/Editar Alertas**.
  3. Utilize o botão do item para alterar o respectivo estado de alerta.

11. Configurar Definições Principais

Pode configurar as definições do produto (incluindo reconfigurar o perfil de utilizador) a partir da janela de Preferências. Para abri-la, faça uma das seguintes acções:

- Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Preferências**.
- Clique com o botão direito do rato no ícone do BitDefender no tabuleiro de sistema e seleccione **Preferências**.

Nota

Para configurar as definições do programa em detalhe, use o interface no Modo Avançado.Para mais informações, por favor consulte "Configuração e Gestão" (p. 59).

As definições estão organizadas por três categorias:

- Opções de Segurança
- Definições de Alertas
- Configuração Geral

Para activar ou desactivar uma definição, utilize o respectivo botão.

Para aplicar e salvar as alterações, clique em **OK**. Para fechar a janela e não salvar as alterações, clique em **Cancelar**.

A hiperligação **Reconfigurar Perfil** no canto superior direito da janela permite-lhe reconfigurar o perfil de utilização.Para mais informação, por favor consulte o "*Reconfigurar o Perfil de Utilização*" (p. 52).

11.1. Opções de Segurança

Aqui, pode activar ou desactivar configurações do produto que abrangem diversos aspectos da segurança do computador e dos dados.Para activar ou desactivar uma definição, utilize o respectivo botão.

Atenção

Tenha cuidado ao desactivar a protecção em tempo-real do antivírus, a firewall ou a actualização automática.Desactivar estas opções pode comprometer a segurança do seu computador. Se realmente necessita de as desactivar, não se esqueça de as activar novamente o mais rapidamente possível.

Estas são as definições disponíveis:

Antivírus

A protecção em tempo-real assegura que todos os ficheiros acedidos por si ou por uma aplicação são analisados.

Actualização Automática
A actualização automática assegura que os produtos e as assinaturas mais recentes da BitDefender são descarregados da Internet e instalados automaticamente numa base regular.As actualizações estão predefinidas para ocorrerem de hora em hora.

Ver Vulnerabilidades
A Análise Automática de Vulnerabilidade alerta-o e ajuda-o a corrigir vulnerabilidades do seu sistema que poderão afectar a segurança. Estas vulnerabilidades incluem software desactualizado, palavras-passe das contas de utilizador fracas ou actualizações do Windows em falta.

Antispam
O Antispam filtra as mensagens de E-mail recebidas, marcando a publicidade não solicidada e o lixo electronico como SPAM.

Antiphishing
A protecção Antiphishing web em tempo-real detecta e alerta-o em tempo-real se uma página web está feita para roubar informação pessoal.

Consultor de Procura
O Consultor de Procura analisa as hiperligações dos resultados das suas pesquisas e indica quais são seguras e quais não são.

Controlo de identidade
O Controlo de Identidade ajuda a impedir que os seus dados pessoais sejam expostos na Internet sem o seu consentimento. Bloqueia todas as mensagens instantâneas, mensagens de e-mail ou outras formas de transmissão de dados pela web que tenha definido como sendo privado para destinatários não autorizados (endereços).

Encriptação de Chat
A Encriptação de Conversa através do Yahoo! Messenger e Windows Live Messenger só é possível se a pessoa de contacto utilizar um produto BitDefender compativel.

Controlo Parental (utilizador actual)
O Controlo Parental restringe o computador e as actividades online das crianças, baseado nas regras que você definiu.As restrições podem incluir o bloqueio de sites de web inadequados, bem como limitar o acesso à Internet e a jogos a um determinado horário.

Firewall
A Firewall protege o seu computador contra os hackers e os ataques maliciosos externos.

Encriptação Ficheiro
O Cofre de ficheiros mantém os seus documentos privados ao encriptá-los em drives de cofre especiais.Se desactivar o Cofre de Ficheiros, todos os cofres de

ficheiros serão fechados e não será mais capaz de aceder aos ficheiros que eles contêm.

O estado de algumas destas definições podem ser monitorizadas pelo sistema de monitorização do BitDefender.Se desactivar a definição de monitorização, o BitDefender irá identicar como incidencia que necessita de der reparada.

Se não desejar que uma definição de monitorização que desactivou seja detectada como Incidência, tem de configurar o sistema de monitorização para tal. Pode fazê-lo no Modo Intermédio ou no Modo Avançado.Para mais informações, por favor consulte *"Configurar os Alertas de Estado"* (p. 46).

11.2. Definições de Alertas

Nesta área, pode desactivar os pop-ups e alertas do BitDefender.BitDefender utiliza alertas para pedir acções e pop-ups para informar sobre acções automaticamente aplicadas ou outros eventos.Para activar ou desactivar uma categoria de alertas, utilize o respectivo botão.

Importante
A maioria destes alertas e pop-ups devem ser activados para evitar potenciais problemas.

Estas são as definições disponíveis:

Alertas Antivírus
Os alertas antivírus notificam quando o BitDefender detecta e bloqueia um vírus.Quando é detectado um vírus, a melhor opção é analisar a totalidade do sistema para garantir que não há mais vírus.

Pop-ups do Controlo Activo de Vírus
Se estiver a utilizar o Modo Básico ou o Modo Intermédio, um pop-up irá aparecer sempre que o Controlo de Vírus Activo bloquear uma aplicação potencialmente prejudicial.Se estiver a utilizar o Modo Avançado, ser-lhe-á pedida uma acção, através de uma janela de alerta, sempre que que uma aplicação apresentar um comportamento malicioso.

Analisar pop-ups de correio electrónico
Estes pop-ups são mostrados para informar que o BitDefender está a analisar a presença de malware nas mensagens electrónicas.

Alertas da gestão de Rede Pessoal
Estes alertas informam o utilizador quando estão a ser efectuadas acções administrativas à distância.

Pop-ups da firewall
A firewall utiliza pop-ups para informar sobre os vários eventos relacionados com a sua ligação de rede (por exemplo, quando um novo computador liga à sua rede sem fios, quando uma aplicação é autorizada a aceder à Internet ou

quando é bloqueada uma análise de porta).Se estiver a utilizar o Modo Avançado, ser-lhe-á pedida uma acção, através de uma janela de alerta, sempre que que uma aplicação desconhecida tentar ligar à Internet.

Estes pop-ups poderão ser úteis para detectar tentativas de intrusão e proteger a sua rede contra ameaças.

Alertas da Quarentena
Os alertas de quarentena informam quando são eliminados ficheiros antigos da quarentena.

Alertas do Controlo Parental
Sempre que o Controlo Parental bloqueia uma actividade, é apresentado um alerta a informar o utilizador por que é que a actividade está a ser bloqueada (por exemplo, é apresentada uma página da Internet com alerta em vez da página que foi bloqueada).

Pop-us de Registo
Os pop-ups de registo são utilizados para lembrar que tem de registar o BitDefender ou para informar que a chave de licença está quase a expirar ou já expirou.

11.3. Configuração Geral

Aqui, pode activar ou desactivar as definições referentes ao produto e à experiencia do utilizador.Para activar ou desactivar uma definição, utilize o respectivo botão.

Estas são as definições disponíveis:

Modo de Jogo
O Modo de Jogo modifica temporariamente as definições de segurança de forma a minimizar o seu impacto no desempenho do seu sistema durante o jogo.

Detecção de Modo Portátil
O Modo Portátil modifica temporariamente as definições de segurança de forma a minimizar o seu impacto sobre o tempo de vida da bateria do seu portátil.

Definição de Palavra-passe
Para impedir que outra pessoa altere as definições do BitDefender, pode protegê-las com uma palavra-passe.Quando activar esta opção, será solicitado a configurar as definições de palavra-passe.Insira a palavra-passe desejada nos dois campos e clique em **OK** para definir a palavra-passe.

Notícias BitDefender
Ao activar esta opção, irá receber notícias importantes sobre a empresa BitDefender, sobre as actualizações do produto ou sobre novas ameaças de segurança.

Alertas de Notificação do Produto
Ao activar esta opção, irá receber alertas de informação.

Barra de Actividade da Análise
: A barra de actividade da análise é uma janela pequena, transparente, que indica o progresso da actividade da análise do BitDefender.

Enviar relatórios de vírus
: Ao activar esta opção, os relatórios das análises são enviados para o Laboratório BitDefender para análise. Estes relatórios não contém qualquer informação considerada pessoal e confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial.

Detecção de Surtos
: Ao activar esta opção, os relatórios relativos a potenciais surtos de vírus são enviados para o Laboratório BitDefender para análise. Estes relatórios não contém qualquer informação considerada pessoal e confidencial (tal como o nome, endereço IP, etc) e não serão usados para qualquer propósito comercial.

11.4. Reconfigurar o Perfil de Utilização

Durante a instalação, poderá configurar um perfil de utilização.O perfil de utilização reflecte as principais actividades desenvolvidas no computador. Dependendo do perfil de utilização, a interface do produto é organizada para permitir o acesso fácil às suas ferramentas preferidas.

Para reconfigurar o perfil de utilização, clique em **Reconfigurar Perfil** e siga o assistente de configuração.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Escolha o seu Modo**

   Seleccione o modo de interface preferido.

2. **Configurar as Ferramentas**

   Se tiver seleccionado o Modo Básico ou o Modo Intermédio, escolha os recursos para os quais deseja criar atalhos no Painel de Instrumentos.

3. **Configurar Definições**

   Se tiver seleccionado o Modo Avançado, configure as definições BitDefender consoante o necessário.Para activar ou desactivar uma definição, utilize o respectivo botão.

4. **Configurar o Controlo Parental**

   Nota
   Este passo só aparece se tiver adicionado o Controlo Parental aos Meus Instrumentos.

   Pode seleccionar uma das três opções:

   - **Definir o Controlo Parental nas contas dos filhos**

Seleccione esta opção para activar o Controlo Parental nas contas do Windows criadas para os seus filhos e gerir a partir da conta de administrador.

- **Definir o Controlo Parental na conta actual**

  Seleccione esta opção para activar o Controlo Parental na conta do Windows actual. Isto significa que não terá de criar contas separadas para os seus filhos, mas as regras do Controlo Parental irão afectar todas as pessoas que utilizem esta conta.

  Neste caso, é necessária uma palavra-passe para proteger as definições do Controlo Parental.Pode definir agora ou mais tarde a partir da janela do BitDefender.

- **Saltar a configuração por agora**

  Seleccione esta opção para configurar este recurso mais tarde na janela do BitDefender.

5. **Gestão da Rede Pessoal**

Nota
Este passo só aparece se tiver adicionado a Gestão de Rede Doméstica aos Meus Instrumentos.

Pode seleccionar uma das três opções:

- **Definir este PC como "Servidor"**

  Seleccione esta opção se pretende gerir os produtos BitDefender noutros computadores da rede doméstica a partir deste.

  É necessária uma palavra-passe para entrar na rede.Introduza nas respectivas caixas de texto e clique em **Submeter**.

- **Definir este PC como "Cliente"**

  Seleccione esta opção se o BitDefender será gerido a partir de outro computador da rede doméstica que também tem o BitDefender instalado.

  É necessária uma palavra-passe para entrar na rede.Introduza a palavra-passe nas respectivas caixas de texto e clique em **Submeter**.

- **Saltar a configuração por agora**

  Seleccione esta opção para configurar este recurso mais tarde na janela do BitDefender.

6. **Configuração Concluída**

Clique em **Terminar**.

12. Histórico e Eventos

O link **Histórico** no fundo da janela principal do BitDefender abre uma outra janela com o histórico dos & eventos. Esta janela oferece uma visão geral dos eventos relacionados com a segurança.Por exemplo, pode verificar facilmente se a actualização foi levada a cabo com sucesso, se foi encontrado malware no seu computador, se as suas tarefas de backup se executaram sem erros, etc.

De forma a ajudá-lo a filtrar o histórico dos & eventos BitDefender, as seguintes categorias são apresentadas do lado esquerdo:

- **Painel**
- **Antivírus**
- **Antispam**
- **Controlo Parental**
- **Controlo de Privacidade**
- **Firewall**
- **Vulnerabilidade**
- **Backup**
- **Encriptação de Conversa**
- **Encriptação Ficheiro**
- **TUNE-UP**
- **Modo Jogo/Portátil**
- **A Sua Rede**
- **Actualização**
- **Registo**

Está disponível uma lista de eventos para cada categoria. Cada evento vem com a seguinte informação: uma breve descrição, a acção que o BitDefender tomou e quando aconteceu, e a data e hora em que ocorreu. Se deseja saber mais informação acerca de um evento em particular da lista, faça duplo clique sobre esse evento.

Aqui também pode ver os detalhes e as estatísticas relativamente aos eventos do Controlo Parental, tais como os sítios de Internet visitados ou as aplicações utilizadas pelos seus filhos.

Clique em **Limpar Log** se deseja remover antigos logs ou **Actualizar** para se certificar que os logs mais recentes são mostrados.

13. Registo e a Minha Conta

O Registo é um processo de dois passos:

1. **Activação do produto (registo de uma conta BitDefender).** Deve de criar uma conta BitDefender de forma a receber actualizações e a ter acesso a suporte técnico gratuito.Se já tem uma conta BitDefender, registe o seu produto BitDefender nessa conta.O BitDefender irá avisá-lo que necessita de activar o seu produto e ajudá-lo-á a reparar essa incidência.

Importante

Tem de criar uma conta no prazo de 15 dias depois de instalar o BitDefender.De outra forma, o BitDefender deixa de ser actualizado.

2. **Registo com uma chave de licença.** A chave de licença especifica durante quanto tempo está autorizado a usar o produto.Assim que a chave de licença expira, o BitDefender pára de executar as suas funções e de proteger o seu computador.Deve de adquirir uma chave de licença ou renovar a sua licença uns dias antes da actual licença expirar.

Se adquiriu o BitDefender Total Security 2011 num CD/DVD ou em linha, foi-lhe pedido que registasse o seu produto com uma chave de licença durante a instalação.

Se transferiu o BitDefender Total Security 2011 para avaliação, tem de registar o produto com uma chave de licença para continuar a utilizá-lo após o período de avaliação de 30 dias.Durante o período de testes, o produto é 100% funcional e pode testá-lo de forma a ver se está de acordo com as suas expectativas.

13.1. Registar BitDefender Total Security 2011

Se quer registar o produto com uma chave de licença ou alterar a sua chave de licença actual, clique na hiperligação **Informação de Licença**, localizado no fundo da janela do BitDefender.Irá aparecer a janela de registo de produto .

Pode ver o estado do registo do BitDefender, a actual chave de licença e quantos dias faltam para a licença expirar.

Para registar BitDefender Total Security 2011:

1. Insira a chave de licença no campo de edição.

Nota

Pode encontrar a sua chave de licença:

- Na bolsa do CD.
- ou no cartão de registo do produto.
- no e-mail da sua compra on-line.

Se não possuir uma chave de licença BitDefender, clique na hiperligação disponibilizada para iniciar o assistente que o irá ajudar a adquirir uma.

2. Clique em **Registar Agora**.
3. Clique em **Terminar**.

13.2. A activar o BitDefender

Para activar o BitDefender, necessita de criar, ou entrar numa conta BitDefender.Se não registou uma conta BitDefender durante o assistente de instalação, pode fazê-lo da seguinte forma:

Modo Básico
: Clique em **Ver Todas as Incidências**.O assistente irá ajudá-lo a corrigir todas as incidências pendentes, incluindo a activação do produto.

Modo Intermédio
: Vá ao separador **Segurança** e clique no botão **Ver & Corrigir** relacionado com o problema de actualização do produto.Clique em **Iniciar** na janela do assistente para activar o produto.

Modo Avançado
: Vá a **Registo** e clique no botão **Activar Produto**.

Irá abrir a janela de registo de conta.Aqui pode criar ou entrar em uma conta Bitdefender para activar o produto.

Se não deseja criar uma conta BitDefender neste momento, seleccione **Criar Conta Mais Tarde** e clique em **Concluir**.De outra forma, actue de acordo com a sua presente situação:

- "Não tenho uma conta BitDefender" (p. 56).
- "Já tenho uma conta BitDefender" (p. 57).

Importante

Tem de criar uma conta no prazo de 15 dias depois de instalar o BitDefender.De outra forma, o BitDefender deixa de ser actualizado.

Não tenho uma conta BitDefender

Para criar uma conta BitDefender com sucesso, siga estes passos:

1. Seleccione **Criar uma nova conta**.
2. Digite as informações solicitadas nos campos correspondentes.Os dados que nos fornecer serão mantidos confidenciais.
   - **Nome de utilizador** - insira o seu endereço electrónico.
   - **Palavra-passe** - insira uma palavra-passe para a sua conta BitDefender.A palavra-passe tem de ter entre 6 e 16 caracteres de tamanho.

- **Re-inserir a palavra-passe** - inserir novamente a palavra-passe previamente definida.

  Não tem de escrever novamente a palavra-passe se seleccionar não ocultar a palavra-passe enquanto escreve.
- **Dica da Palavra-Passe** - introduza uma palavra ou frase que ajude a relembrar a palavra-passe no caso de a esquecer.

Nota
Uma vez com a conta activada, poderá utilizar o endereço de e-mail fornecido e a palavra-passe para entrar na sua conta em http://myaccount.bitdefender.com.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta.Clique em **Ver Opções de Contacto** e seleccione uma das opções disponíveis na janela que aparece.
   - **Envie-me todas as mensagens**
   - **Enviar mensagens importantes**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Submeter**.
5. Clique em **Concluir** para fechar a janela.

Nota
Antes de usar a sua conta, tem de a activar.
Verifique o seu e-mail e siga as instrucções da mensagem de e-mail que o serviço de registo BitDefender lhe enviou.

Já tenho uma conta BitDefender

O BitDefender detectará automaticamente se já registou previamente uma conta BitDefender no seu computador.Nesse caso, forneça a palavra-passe da sua conta e clique em **Submeter**.Clique em **Concluir** para fechar a janela.

Se já tiver uma conta activada mas o BitDefender não a detecta, siga estes passos para registar essa conta ao produto:

1. Seleccione **Entrar (Conta Existente)**.
2. Digite o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes.

Nota
Se não se lembra da sua palavra-passe, clique em **Esqueceu a sua palavra-passe?** e siga as instruções.

3. Opcionalmente, a BitDefender pode informá-lo acerca de ofertas especiais e promoções usando o endereço de e-mail da sua conta.Clique em **Ver Opções de Contacto** e seleccione uma das opções disponíveis na janela que aparece.
   - **Envie-me todas as mensagens**
   - **Enviar mensagens importantes**
   - **Não me enviem quaisquer mensagens**
4. Clique em **Submeter**.
5. Clique em **Concluir** para fechar a janela.

13.3. Adquirir ou Renovar Chaves de Licença

Se o período de testes vai terminar em breve, deve de adquirir uma chave de licença e registar o seu produto.

De igual modo, se a sua actual chave de licença vai expirar brevemente, deve renová-la.Como cliente BitDefender, você beneficia de um desconto quando renovar a sua licença BittDefender. Pode também mudar de versão do seu produto com um desconto especial ou mesmo inteiramente grátis.

Para iniciar um procedimento simples e seguro, com quatro passos, que irá permitir adquirir uma nova chave ou renovar uma já existente, abra o BitDefender no Modo Intermédio ou no Modo Avançado e clique na hiperligação **Comprar** / **Renovar** ao fundo da janela.

Configuração e Gestão

14. Configuração Geral

O módulo Geral dá-lhe informação sobre a actividade do BitDefender e do sistema.Aqui é onde pode modificar o comportamento global do BitDefender.

Para configurar as definições gerais:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Geral > Definições**.

- **Activar protecção das configurações por palavra-passe** - activa a definição de uma palavra-passe de forma a proteger a configuração do BitDefender.

Nota
Se não for a única pessoa a utilizar este computador, recomendamos que protega as suas configurações do BitDefender com uma palavra-passe.

Introduza a palavra-passe no campo **Palavra-role="passe**, insira-a novamente no campo **Inserir de novo** e clique em **OK**.

Uma vez que tenha definido a palavra-passe, será solicitado que a insira sempre que deseje alterar as configurações do BitDefender.Os outros administradores de sistema (se existirem) também terão de inserir a palavra-passe se desejarem alterar as configurações do BitDefender.

Se desejar ser notificado para inserir a palavra-passe apenas quando configurar o Controlo Parental, deverá também seleccionar **Aplicar palavra-passe apenas para as definições do Controlo Parental**.Por outro lado, se uma palavra-passe for definida apenas para o Controlo Parental e deseleccionar essa opção, a palavra-passe respectiva será requisitada quando configurar qualquer opção do BitDefender.

Importante
Se se esqueceu da palavra-passe, terá de reparar o produto para que possa modificar a configuração do BitDefender.

- **Perguntar se quero criar uma palavra-passe ao activar o Controlo Parental** - pede-lhe que defina uma palavra-passe quando activar o Controlo Parental e não houver uma definida.Ao definir uma palavra-passe, irá prevenir que outros utilizadores com direitos administrativos possam mudar as suas definições do Controlo Parental que configurou para um determinado utilizador.
- **Mostrar Notícias BitDefender (notificações de segurança)** - mostra de tempos em tempos, notificações de segurança relacionadas com epidemias de vírus, enviadas pelo servidor do BitDefender.

- **Mostrar pop-ups (notas no ecrã)** - apresenta uma janela de pop-up no windows que mostra o estado do produto.Pode configurar o BitDefender para exibir pop-ups apenas quando o interface está no Modo Básico / Intermédio ou no Modo Avançado.
- **Mostra a barra de Actividade da Análise (gráfico no ecrã da actividade do produto)** - Exibe a barra de Actividade da Análisesempre que entrar no Windows.Limpe esta caixa se deseja que a barra de Actividade da Análise não seja mostrada daí em diante.

Nota

Esta opção pode ser configurada apenas para a actual conta de utilizador Windows.A barra de actividade da análise só está disponível no Modo Avançado.

Configuração do Relatório de Vírus

- **Enviar relatórios de vírus** - envia relatórios que contêm vírus identificados no seu computador para os Laboratórios do BitDefender. Ajuda-nos a seguir o rasto das quebras dos vírus.

  Os relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e não serão usados com fins comerciais. A informação fornecida irá conter apenas o nome do vírus e será usada, somente para criar relatórios estatísticos.
- **Activar Detecção de Epidemias BitDefender** - envia relatórios para os Laboratórios do BitDefender com respeito a potenciais epidemias de vírus.

  Os relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e não serão usados para fins comerciais. A informação fornecida contém apenas o potencial vírus e será usada somente para ajudar a detectar novos vírus.

Definições de Ligação

Vários componentes do BitDefender (os módulos de Firewall, LiveUpdate, Notificação de Vírus em Tempo Real e Notificação de Spam em Tempo Real) requerem acesso à Internet. O BitDefender possui um gestor de proxy que permite a configuração a partir de uma localização das definições de proxy utilizadas pelos componentes do BitDefender para aceder à Internet.

Se a sua empresa usa um servdior proxy para se ligar à Internet, deverá especificar as definições do proxy de forma a que o BitDefender se actualize sozinho. De outra forma, usará as definições do administrador que instalou o produto ou o utilizador actual por defeito do browser, caso haja algum.Para mais informação, por favor consulte o *“Como Posso Encontrar as Minhas Definições de Proxy?”* (p. 262).

Nota
As definições do proxy só podem ser configuradas por utilizadores com direitos administrativos no computador ou por power users (utilizadores que sabem a palavra-passe da configuração do produto).

Para gerir as definições proxy, clique em **Definições Proxy**.

Existem três categorias de definições de proxy:

- **Proxy detectado durante o Período de Instalação)** - as definições de proxy detectadas na conta de administrador durante a instalação e que podem ser configuradas apenas se estiver com sessão iniciada nessa conta. Se o servidor proxy requer um nome de utilizador e uma palavra-passe, deverá inseri-los nos campos correspondentes.
- **Browser por Defeito do Proxy** - as definições do proxy do actual utilizador, extraídas do browser por defeito. Se o servidor proxy requer um nome de utilizador e uma palavra-passe, deve de os inserir nos campos correspondentes.

Nota
Os browsers de internet suportados são o Internet Explorer, Mozilla Firefox e Opera. Se utiliza outro explorador por defeito, o BitDefender não será capaz de obter as definições do proxy do actual utilizador.

- **Personalizar Proxy** - definições de proxy que pode configurar se estiver logged in como administrador.

  As seguintes definições devem ser especificadas:
  - **Endereço** - introduza o IP do servidor proxy.
  - **Porta** - insira a porta que o BitDefender usa para se ligar ao servidor proxy.
  - **Nome de Utilizador** - introduza um nome de utilizador reconhecido pelo proxy.
  - **Palavra-passe** - introduza uma palavra-passe válida para o utilizador previamente definido.

O BitDefender utilizará os grupos de definições proxy na seguinte ordem até conseguir ligação à Internet:

1. as definições proxy especificadas.
2. as definições proxy detectadas no momento da instalação.
3. as definições proxy do actual utilizador.

Quando tentar ligar-se à Internet, cada conjunto de definições do proxy é experimentado na sua vez, até que o BitDefender se consiga ligar.

Primeiro, o conjunto que contém as suas definições do proxy será utilizado para ligar a Internet. Se esse não funcionar, as definições de proxy detectadas durante a instalação serão experimentadas logo a seguir. Finalmente se nenhuma dessa funcionar, as definições de proxy do utilizador actual serã retiradas do seu browser por defeito e usadas para obter a ligação à Internet.

Clique em **OK** para guardar as alterações e fechar a janela.

Clique em **Aplicar** para guardar as alterações, ou clique em **Defeito** para retornar às definições por defeito.

Informação do Sistema

BitDefender permite-lhe visualizar, a partir de uma única localização, todas as configurações do sistema e as aplicações registadas para se executarem durante o iniciar do Windows. Desta forma, pode gerir a actividade da seu sistema e as aplicações instaladas nele como também identificar possíveis infecções.

Para obter a informação do sistema:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Geral > Informação do Sistema**.

A lista contém todos os itens carregados quando inicia o sistema assim como os itens carregados pelas diferentes aplicações.

Estão disponíveis três botões:

- **Restaurar** - muda a actual associação de ficheiros para o modo por defeito.Disponível apenas para as definições das **Associações de Ficheiros**!
- **Ir para** - abre uma janela onde o item seleccionado é colocado (o **Registo** por exemplo).

Nota
Dependendo do item seleccionado o botão **Ir Para** poderá não aparecer.

- **Actualizar** - reabre a secção de **Info Sistema**.

15. Protecção Antivírus

BitDefender protege o seu computador de todo o tipo de malware (vírus, Trojans, spyware, rootkits e por aí fora).A protecção que BitDefender oferece está dividida em duas categorias:

- Protecção em Tempo-real - previne que novas ameaças de malware entrem no seu sistema.Poe exemplo, BitDefender irá analisar um documento word em busca de ameaças conhecidas quando você o abrir, e uma mensagem de e-mail quando recebe uma.

  A protecção em Tempo-real, também referida como análise no-acesso - os ficheiros são analisados à medida que os utilizadores lhes acedem.

  Importante
  Para prevenir que o seu computador seja infectado por vírus mantenha activa a **Protecção em Tempo-real**.

- Análise a-pedido - permite detectar e remover malware que já se encontra a residir no seu sistema.Esta é uma análise clássica iniciada pelo utilizador – você escolhe qual a drive, pasta ou ficheiro o BitDefender deverá analisar, e o mesmo é analisado – a-pedido.A tarefa de análise permite que crie rotinas personalizadas de análise e elas podem ser agendadas para serem executadas numa base regular.

Quando detecta um vírus ou outro malware, o BitDefender irá tentar remover automaticamente o código de malware do ficheiro e reconstruir o ficheiro original.Esta operação é designada por desinfecção.Os ficheiros que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção.Para mais informação, por favor consulte o “*Área de Quarentena*” (p. 86).

Se o seu computador estiver infectado com malware, por favor consulte “*Remover Malware do Sistema*” (p. 244).

Os utilizadores avançados podem configurar as exclusões da análise se não quiserem que certos ficheiros sejam analisados.Para mais informação, por favor consulte o “*Configurar Exclusões da Análise*” (p. 83).

15.1. Protecção em Tempo-real

O BitDefender providencia uma protecção contínua e em tempo-real, contra todo o tipo de ameaças de malware ao analisar os ficheiros acedidos, e as comunicações feitas através de aplicações de software de Mensagens Instantâneas (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

As predefinições da protecção em tempo real asseguram uma óptima protecção contra malware, com um impacto mínimo no desempenho do seu sistema.Pode alterar facilmente as definições da protecção em tempo real de acordo com as suas

necessidades mudando para um dos níveis de protecção predefinidos.Ou, no modo avançado, pode configurar as definições de análise em detalhe criando um nível de protecção personalizado.

Para saber mais, consulte os seguintes tópicos:

- *"Ajustar o Nível de Protecção em Tempo Real"* (p. 65)
- *"Criar um Nível de Protecção Personalizado"* (p. 66)
- *"Alterar as Acções Aplicadas aos Ficheiros Detectados"* (p. 67)
- *"Restaurar as Predefinições"* (p. 68)

Para proteger o seu sistema contra aplicações maliciosas desconhecidas, o BitDefender utiliza uma avançada tecnologia heurística (Controlo de Vírus Activo) e um Sistema de Detecção de Intrusão, que monitorizam constantemente o seu sistema.Para saber mais, consulte os seguintes tópicos:

- *"Configurar o Controlo Activo de Vírus"* (p. 69)
- *"Configurar o Sistema de Detecção de Intrusão:"* (p. 71)

15.1.1. Ajustar o Nível de Protecção em Tempo Real

O nível de protecção em tempo real determina as definições de análise da protecção em tempo real.Pode alterar facilmente as definições da protecção em tempo real de acordo com as suas necessidades mudando para um dos níveis de protecção predefinidos.

Para ajustar o nível de protecção em tempo real:

1. Abrir o BitDefender.
2. Dependendo do modo de interface do utilizador, proceda da seguinte forma:

   Modo Intermédio

   Abra o separador **Segurança** e clique em **Configurar o Antivírus**, nas Tarefas Rápidas, no lado esquerdo da janela.

   Abra o separador **Escudo**.

   Modo Avançado

   Vá a **Antivírus > Escudo**.

Nota

No Modo Básico e no Modo Intermédio, pode configurar um atalho para poder aceder a estas definições a partir do painel de instrumentos.Para mais informação, por favor consulte o *"Ferramentas"* (p. 36).

3. Arraste o cursor pela escala para definir o nível de protecção pretendido.Utilize a descrição do lado direito da escala para escolher o nível de protecção que melhor se adequa às suas necessidades de segurança.

15.1.2. Criar um Nível de Protecção Personalizado

Os utilizadores avançados poderão querer tirar partido das configurações de análise que o BitDefender oferece. O analisador pode ser configurado para evitar extensões de ficheiros, directorias ou arquivos que sabe serem inofensivos. Isto poderá reduzir o tempo de análise e melhorar a resposta do seu computador durante uma análise.

Pode configurar as definições da protecção em tempo real criando um nível de protecção personalizado.Para criar um nível de protecção personalizado:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Personalizar Nível**.
4. Configure as definições de análise como necessário.Para saber o que uma opção faz, mantenha o rato sobre a mesma e leia a descripção apresentada no fundo da janela.
5. Clique em **OK** para guardar as alterações e fechar a janela.

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no glossário.Pode também encontrar informação útil pesquisando a Internet.
- **Analisar ficheiros acedidos.** Pode definir o BitDefender para analisar todos os ficheiros acedidos, apenas aplicações (ficheiros de programa) ou tipos de ficheiro específicos que achar perigosos.A análise de todos os ficheiros acedidos proporciona uma maior segurança, enquanto a análise apenas das aplicações pode ser utilizada para melhorar o desempenho do sistema.

  As aplicações (ou ficheiros de programa) são muito mais vulneráveis a ataques de malware do que qualquer outro tipo de ficheiros.Esta categoria inclui as seguintes extensões de ficheiro:`.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  Se optar por **Analisar extensões definidas pelo utilizador**, é recomendado que inclua todas as extensões de aplicação para além das extensões de ficheiros que considere perigosas.

- **Analisar só ficheiros alterados.** Ao analisar apenas ficheiros novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.
- **Analisar dentro dos arquivos.** Analisar o interior de arquivos é um processo lento e que consome muitos recursos, não sendo, por isso recomendado para a protecção em tempo real.Os arquivos que contém ficheiros infectados não são uma ameaça imediata à segurança do seu sistema.O malware só pode afectar o seu sistema se o ficheiro infectado for extraído do arquivo e executado sem que a protecção em tempo real esteja activada.
- **Opções de acção.** Se pretender alterar as acções aplicadas a ficheiros detectados, procure dicas em *"Alterar as Acções Aplicadas aos Ficheiros Detectados"* (p. 67).
- **Opções de análise para tráfego de correio electrónico, Internet e mensagens instantâneas.** Para impedir que seja transferido malware para o seu computador, o BitDefender analisa automaticamente os seguintes pontos de entrada de malware:
  - correio recebido
  - tráfego da Internet
  - ficheiros recebidos através do Yahoo! Messenger e Windows Live Messenger

  Analisar o tráfego na Internet poderá abrandar um pouco a navegação, mas vai bloquear o malware proveniente da Internet, incluindo transferências "drive-by".

  Apesar de não ser recomendado, pode desactivar a análise ao correio electrónico, Internet ou mensagens instantâneas para aumentar o desempenho do sistema.Se desactivar as respectivas opções de análise, as mensagens electrónicas e os ficheiros recebidos e transferidos da Internet não serão analisados, permitindo que ficheiros infectados sejam guardados no seu computador.Esta é uma ameaça grave pois a protecção em tempo real vai bloquear o malware quando os ficheiros infectados forem acedidos (abertos, movidos, copiados ou executados).

15.1.3. Alterar as Acções Aplicadas aos Ficheiros Detectados

Os ficheiros detectados pela protecção em tempo real são agrupados em duas categorias:

- **Ficheiros infectados.** Os ficheiros detectados como infectados correspondem a uma assinatura de malware na Base de Dados de Assinaturas de Malware do BitDefender.Por norma, o BitDefender consegue remover o código de malware de um ficheiro infectado e reconstruir o ficheiro original. Esta operação é conhecida por desinfecção.

Nota

As assinaturas de malware são fragmentos de código extraídos de amostras de malware. São utilizados por programas antivírus para efectuar correspondência entre padrões e detectar malware.

A Base de Dados de Assinatura de Malware BitDefender é uma colecção de assinaturas de malware actualizada a toda hora pelos investigadores de malware da BitDefender.

- **Ficheiros suspeitos.** Os ficheiros são detectados como suspeitos pela análise heurística.Não foi possível desinfectar os ficheiros suspeitos por não estar disponível uma rotina de desinfecção.

Consoante o tipo do ficheiro detectado, são tomadas automaticamente as seguintes acções:

- Se for detectado um ficheiro infectado, o BitDefender tentará automaticamente desinfectá-lo.Se a desinfecção falhar, o ficheiro é movido para a quarentena de modo a restringir a infecção.

Importante

Para determinados tipos de malware, a desinfecção não é possível por o ficheiro detectado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

- Se for detectado um ficheiro suspeito, o acesso a esse ficheiros será impedido para impedir uma potencial infecção.

Não deve alterar a acções predefinidas aplicadas aos ficheiros detectados excepto se tiver uma forte razão para isso.

Para alterar as acções predefinidas aplicadas aos ficheiros infectados ou suspeitos detectados:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Personalizar Nível**.
4. Configure as acções a aplicar em cada categoria de ficheiros detectados, consoante o necessário.A segunda acção é aplicada se a primeira falhar (por exemplo, se não for possível desinfectar, o ficheiro infectado é movido para a quarentena).

15.1.4. Restaurar as Predefinições

As predefinições da protecção em tempo real asseguram uma óptima protecção contra malware, com um impacto mínimo no desempenho do seu sistema.

Para restaurar as definições da protecção em tempo real:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.

2. Vá a **Antivírus > Escudo**.
3. Clique em **Nível Predefinido**.

15.1.5. Configurar o Controlo Activo de Vírus

O Controlo de Vírus Activo BitDefender detecta aplicações potencialmente destrutivas baseado no seu comportamento.

O Controlo de Vírus Activo monitoriza as aplicações executados no computador, procurando acções identificáveis como malware. Cada uma destas acções é classificada e é calculada uma pontuação geral para cada processo.Quando a pontuação geral de um processo atinge um determinado limite, o processo é considerado prejudicial. Consoante as definições do programa, o processo é automaticamente bloqueado ou poder ser-lhe pedido que indique a acção a aplicar.

O Controlo Activo de Vírus pode ser configurado para o alertar e pedir-lhe para agir sempre que uma aplicação tentar executar umas acção possivelmente maliciosa.

Se conhece e confia na aplicação detectada, clicque em **Permitir**.

Se deseja fechar imediatamente a aplicação, clique em **OK**.

Seleccione a caixa de selecção **Lembrar esta acção para esta aplicação** antes de fazer a sua escolha e o BitDefender tomará a mesma acção no futuro para a aplicação detectada.A regra que é então criada será listada na janela da configuração do Controlo Activo de Vírus.

Para configurar o Controlo Activo de Vírus:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Configuração Avançada**.
4. Abra o separador **AVC**.
5. Seleccione a marca da caixa correspondente para activar o Controlo Activo de Vírus.
6. Arraste o cursor pela escala para definir o nível de protecção pretendido.Utilize a descrição do lado direito da escala para escolher o nível de protecção que melhor se adequa às suas necessidades de segurança.

Ajustar o Nível de Agressividade

Para configurar o nível de protecção do Controlo de Vírus Activo:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.

3. Clique em **Configuração Avançada**.
4. Abra o separador **AVC**.
5. Arraste o cursor pela escala para definir o nível de protecção pretendido.Utilize a descrição do lado direito da escala para escolher o nível de protecção que melhor se adequa às suas necessidades de segurança.

Configurar a Resposta a Comportamento Malicioso

Se uma aplicação apresentar um comportamento malicioso, ser-lhe-á perguntado se quer permitir ou bloquear.

Para configurar a resposta a comportamento malicioso:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Configuração Avançada**.
4. Abra o separador **AVC**.
5. Se quiser receber pedidos de acção quando o Controlo de Vírus Activo detecta uma aplicação potencialmente maliciosa, seleccione a caixa **Alertar-me antes de aplicar qualquer acção**.Para bloquear automaticamente uma aplicação que apresenta um comportamento malicioso (sem apresentar uma janela de alerta), desmarque esta caixa.

Gerir a Lista de Aplicações Confiáveis/Não Confiáveis

Pode adicionar aplicações, que sabe que são fiáveis, à ista de aplicações fiáveis. Essas aplicação não serão mais analisadas pelo Controlo Activo de Vírus do BitDefender e será automaticamente permitido o acesso.

Para gerir as aplicações que não estão a ser monitorizadas pelo Controlo Activo de Vírus:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Configuração Avançada**.
4. Abra o separador **AVC**.
5. Clique no separador **Exclusões**.

As aplicações para as quais criou regras estão listadas na tabela **Exclusões**.O caminho para a aplicação e a acção que definiu para ela (Permitido ou Bloqueado) é exibido para cada regra.

Para alterar uma acção para uma aplicação, faça clique na actual acção e seleccione a outra acção a partir do menu.

Para gerir a lista, utiize os botões que se encontram por cima da tabela:

- **Adicionar** - adiciona uma nova aplicação à lista.
- **Remover** - remove uma aplicação da lista.
- **Editar** - Edita uma regra de uma aplicação.

15.1.6. Configurar o Sistema de Detecção de Intrusão:

O Sistema de Detecção de Intrusão BitDefender supervisiona as actividades da rede e do sistema à procura de comportamentos maliciosos ou violações de privacidade.

Para configurar o Sistema de Detecção de Intrusão:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Configuração Avançada**.
4. Abra o separador **IDS**.
5. Seleccione a caixa respectiva para activar o Sistema de Detecção de Intrusão.
6. Arraste o cursor pela escala para definir o nível de agressividade pretendido.Utilize a descrição do lado direito da escala para escolher o nível de agressividade que melhor se adequa às suas necessidades de segurança.

15.2. Análise a-pedido

O objectivo principal do BitDefender é manter o seu computador livre de vírus. Isto é inicialmente e essencialmente feito, mantendo novos vírus fora do seu computador e ao examinar as suas mensagens de e-mail e novos ficheiros descarregados ou copiados para o seu sistema.

Há o risco de o vírus já ter acedido ao seu sistema, antes mesmo de ter instalado o BitDefender. Este é o motivo, pelo qual é uma excelente ideia verificar vírus residentes no seu computador depois de instalar o BitDefender. E é defenitivamente uma boa ideia, a verificação frequente de vírus no seu computador.

A análise a-pedido está baseada em tarefas de análise. As tarefas de análise especificam as opções de análise e os objectos a serem analisados.Pode analisar o computador sempre que desejar ao executar as tarefas de análise por defeito ou as suas próprias tarefas de análise (tarefas definidas pelo utilizador). Pode também agendá-las para que se executem numa base regular ou quando o sistema está sem ser usado de forma a não interferir com o seu trabalho.Para instruções rápidas, por favor consulte os seguintes tópicos:

- “*Como Posso Analisar Ficheiros e Pastas?*” (p. 208)

- *“Como Posso Criar Uma Tarefa de Análise Personalizada?”* (p. 211)
- *“Como Posso Agendar uma Análise ao Computador?”* (p. 213)

15.2.1. Analisar Ficheiros e Pastas

Deve analisar os ficheiros e as pastas sempre que suspeitar de uma infecção.Clique com o botão direito do rato sobre o ficheiro ou pasta que pretende analisar e seleccione **Analisar com o BitDefender**.O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise.

Se quer analisar localizações específicas no seu computador, pode configurar e executar uma tarefa de análise personalizada.Para mais informação, por favor consulte o *“Como Posso Criar Uma Tarefa de Análise Personalizada?”* (p. 211).

Para analisar o seu computador ou parte dele pode usar as tarefas de análise por defeito ou pode criar as suas próprias tarefas de análise.Para executar uma tarefa de análise, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Básico
: Clique no botão **Segurança** e escolha uma das tarefas de análise disponíveis.

Modo Intermédio
: Vá ao separador **Segurança**.Clique em **Análise Minuciosa ao Sistema** na área de Tarefas Rápidas do lado esquerdo e escolha uma das tarefas de análise disponíveis.

Modo Avançado
: Vá a **Antivírus > Análise de Vírus**.Para levar a cabo uma tarefa de análise do sistema ou definida por si, clique no botão **Executar Tarefa** button.

Estas são as tarefas predefinidas que pode utilizar para analisar o seu computador:

Análise Completa
: Analisa todo o sistema, excepto arquivos.Na configuração por defeito, analisa todos os tipos de malware excepto rootkits.

Análise Rápida
: A Análise Rápida utiliza a análise nas nuvens para detectar malware em execução no seu sistema.Normalmente, a realização de uma Análise Rápida demora menos de um minuto e utiliza uma facção dos recursos do sistema necessários para uma análise de vírus normal.

Análise Minuciosa
: Analisa todo o sistema.Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.

Antes de inciar um processo de análise, deveria certificar-se que o BitDefender está actualizado com as assinaturas de malware mais recentes. Analisar o seu computador

usando assinaturas desactualizadas pode impedir que o BitDefender detecte novo malware encontrado desde a última actualização.

Para que o BitDefender possa efectuar uma verificação completa, tem de encerrar todos os programas abertos. É, especialmente, importante que encerre a sua conta de e-mail (por ex. Outlook, Outlook Express ou Eudora).

Dicas de Análise

Eis aqui mais algumas dicas sobre a análise que lhe poderão ser úteis:

- Dependendo do tamanho do disco rígido, levar a cabo uma análise completa do seu computador (tal como uma Análise Minuciosa ou uma Análise Completa) pode levar algum tempo (uma hora ou mais).Logo, deve de levar a cabo essas análises em momentos em que não necessita do seu computador (por exemplo, durante a noite).

  Pode agendar a análise para começar quando for mais conveniente.Certifique-se de que deixa o seu computador ligado.Com o Windows Vista, certifique-se que o seu computador não está em Modo de Suspensão na altura para a qual a tarefa está agendada.
- Se descarrega frequentemente ficheiros da Internet para uma determinada pasta, crie uma nova tarefa de análise e defina essa pasta como alvo da análise.Agenda a tarefa para correr diariamente ou até com mais frequência.
- Existe um determinado tipo de malware que se prepara para ser executado durante o arranque do sistema ao alterar as definições do Windows.Para proteger o seu computador contra tal tipo de malware, pode agendar a tarefa de **Análise Autologon** para correr durante o iniciar do sistema.Tenha em atenção que a Análise Autologon pode afectar a performance do sistema durante um curto período de tempo após o iniciar do computador.

15.2.2. Assistente de Análise Antivírus

Sempre que inicie uma análise a-pedido (por exemplo, clicar botão direito sobre a pasta e selecionar **Analisar com BitDefender**), o assistente de análise antivírus BitDefender irá aparecer.Siga o processo guiado de três passos para completar o processo de análise.

Nota

Se o assistente de análise não surgir, a análise poderá estar configurada para correr silenciosamente, em segundo plano.Procure pelo ícone do progresso da análise na área de notificação.Pode clicar nesse icone para abrir a janela da análise e ver o seu progresso.

Passo 1/3 - Analisar

BitDefender iniciará a análise dos objectos seleccionados.

Pode ver o estado da análise e as estatisticas (velocidade da análise, tempo decorrido, número de objectos analisados / infectados / suspeitos / ocultos e outras).

Espere que o BitDefender termine a análise.

Nota
O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

Arquivos protegidos com palavra-passe. Quando é detectado um arquivo protegido por palavra-passe, dependendo das definições da análise, poderá ter de indicar a palavra-passe.Os arquivos protegidos por palavra-passe não podem ser analisados a não ser que forneça a palavra-passe.Estão disponíveis as seguintes opções:

- **Quero inserir a palavra-passe para este objecto.** Se quer que o BitDefender analise o arquivo, seleccione esta opção e insira a palavra-passe.Se não sabe a palavra-passe, escolha uma das outras opções.
- **Não quero inserir a palavra-passe para este objecto.** Seleccione esta opção para saltar a análise deste arquivo.
- **Não quero inserir a palavra-passe para nenhum objecto (saltar todos os objectos protegidos por palavra-passe).** Seleccione esta opção se não deseja ser incomodado acerca de arquivos protegidos por palavra-passe.O BitDefender não será capaz de os analisar, mas um registo dos mesmos será mantido no relatório da análise.

Clique em **OK** para continuar a analisar.

Parar ou pausar a análise. Pode parar o processo de análise a qualquer altura que desejar, fazendo clique em **Parar&**. Irá directamente para o último passo do assistente.Para parar temporariamente o processo de análise, clique em **Pausa**. Terá de clicar em**Retomar** para retomar a análise.

Passo 2/3 - Seleccionar as acções

Quando a análise é completada, surge uma nova janela, onde pode ver os resultados da análise.

Se já não houver ameaças por resolver, clique em **Continuar**.Caso contrário, tem de configurar novas acções a aplicar a ameaças não resolvidas para proteger o seu sistema.

Os objectos infectados são apresentados em grupos, baseados no tipo de malware com que estão infectados.Clique no link correspondente a uma ameaça para descobrir mais informação acerca dos objectos infectados.

Pode escolher uma acção geral a ser levada a cabo para todas as incidências ou pode escolher acções separadas para cada grupo de incidências.Uma ou várias das seguintes opções poderão aparecer no menu:

Não Tomar Acção
Nenhuma acção será levada a cabo sobre os ficheiros detectados.Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses ficheiros.

Desinfectar
Remove o código de malware dos ficheiros infectados.

Apagar
Remove os ficheiros detectados do disco.

Mover para a quarentena
Move os ficheiros infectados para a quarentena.O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece.Para mais informação, por favor consulte o *"Àrea de Quarentena"* (p. 86).

Renomear ficheiros
Altera o nome dos ficheiros ocultos ao acrescentar `.bd.ren` ao seu nome.Como resultado, será capaz de procurar e encontrar tais ficheiros no seu computador, se existirem.

Repare que este ficheiros ocultos, não são os ficheiros que esconde deliberadamente no Windows. Eles são ficheiros ocultos por programas especiais, conhecidos como rootkits.Os rootkits não são maliciosos por natureza, No entanto, eles são vulgarmente utilizados para tornar os vírus ou o spyware indetectáveis pelos programas antivírus.

Clique em **Continuar** para aplicar as acções especificadas.

Passo 3/3 - Ver Resultados

Quando o BitDefender termina de reparar estas incidências, o resultado da análise aparecerá numa nova janela.Se deseja uma informação completa sobre o processo de análise, clique em **Mostrar Relatório** para ver o relatório da análise.

Importante
Se necessário, ser-lhe-á solicitado que reinicie o seu computador, para que o processo de limpeza seja completado.

Clique em **Fechar** para fechar a janela.

BitDefender Não Pode Resolver Algumas Incidências

Na maioria dos casos o BitDefender desinfecta com sucesso o ficheiro infectado ou isola a infecção.No entanto, há incidências que não puderam ser automaticamente

resolvidas.Para mais informações e instruções sobre como remover manualmente o malware, por favor consulte “*Remover Malware do Sistema*” (p. 244).

BitDefender Detectou Ficheiros Suspeitos

Ficheiros suspeitos são ficheiros detectados pela análise heurística e que poderão estar infectados com malware cuja a assinatura de detecção ainda não foi disponibilizada.

Se foram detectados ficheiros suspeitos durante a análise, ser-lhe-á solicitado que os envie para o Laboratório do BitDefender.Clique **OK** para enviar estes ficheiros para análise no Laboratório do BitDefender.

15.2.3. Ver os Relatórios da Análise

Sempre que efectuar uma análise, é criado um relatório de análise.O relatório da análise contém informação detalhada acerca dos processos de análise registados, tal como as opções da análise, o alvo da análise, as ameaças encontradas e as acções tomadas sobre essas ameaças.

Pode abrir o relatório directamente no assistente de análise, assim que esta terminar, clicando em **Mostrar Relatório**.

Para consultar os relatórios de análise mais tarde:

1. Abrir o BitDefender.
2. Clique na hiperligação **Ver Relatórios** que se encontra no canto inferior direito da janela.
3. Clique em **Antivirus** do lado esquerdo do menu.
4. Na secção **Tarefas A Pedido**, pode ver as análises que foram recentemente efectuadas.Faça duplo clique nos eventos da lista para ver mais detalhes.Para abrir o relatório da análise, clique em **Ver Relatório de Análise**.O relatório da análise será aberto no seu explorador da internet.

Para eliminar uma entrada de registo, clique nela com o botão direito e seleccione **Eliminar**.

15.2.4. Gerir Tarefas de Análise Existentes

O BitDefender vem com diversas tarefas, criadas por defeito, que cobrem as incidências de segurança mais comuns. Pode também criar as suas próprias tarefas personalizadas.Para mais informação, por favor consulte o “*Como Posso Criar Uma Tarefa de Análise Personalizada?*” (p. 211).

Para gerir tarefas de análise existentes:

1. Abrir o BitDefender.
2. Dependendo do modo de interface do utilizador, proceda da seguinte forma:

Modo Intermédio

Abra o separador **Segurança** e clique em **Configurar o Antivírus**, nas Tarefas Rápidas, no lado esquerdo da janela.

Abra o separador **Análise de Vírus**.

Modo Avançado

Vá a **Antivírus > Análise de Vírus**.

Nota

No Modo Básico e no Modo Intermédio, pode configurar um atalho para poder aceder a estas definições a partir do painel de instrumentos.Para mais informação, por favor consulte o *"Ferramentas"* (p. 36).

Existem três categorias de tarefas de análise:

- **Tarefas do Sistema** - contém a lista das tarefas por defeito do sistema. As seguintes tarefas estão disponíveis:

  Análise Completa

  Analisa todo o sistema, excepto arquivos.Na configuração por defeito, analisa todos os tipos de malware excepto rootkits.

  Análise Rápida

  A Análise Rápida utiliza a análise nas nuvens para detectar malware em execução no seu sistema.Normalmente, a realização de uma Análise Rápida demora menos de um minuto e utiliza uma facção dos recursos do sistema necessários para uma análise de vírus normal.

  Análise Autologon

  Analisar os itens que são executados quando o utilizador entra no Windows.Por defeito, a análise ao logon está desactivada.

  Se deseja usar esta tarefa, faça clique botão direito nela, selecione **Agendar** e defina a tarefa para ser executada no**arranque do sistema**.Pode definir quanto tempo após o iniciar do sistema a tarefa deve de ser iniciada.

  Análise Minuciosa

  Analisa todo o sistema.Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.

Nota

Um vez que as atrefas **Análise Minuciosa do Sistema** e **Análise Completa do Sistema** analisam todo o sistema, a análise deverá demorar um pouco. Por isso, recomendamos que execute estas tarefas com baixa prioridade ou, melhor, quando o seu sistema estiver inactivo.

- **Tarefas do Utilizador** - contém as tarefas definidas pelo utilizador.

Uma tarefa chamada `Os Meus Documentos` é fornecida.Use esta tarefa para analisar pastas de utilizadores actuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de trabalho segura e aplicações limpas a serem executadas no arranque.

- **Tarefas Misc** - contém uma lista de tarefas de análise variadas. Estas tarefas de análise dizem respeito a tipos de análise alternativas que não podem ser executadas a partir desta janela. Apenas pode modificar as suas configurações ou ver os relatórios de análise.As seguintes tarefas estão disponíveis:

Análise de Dispositivos

O BitDefender pode detectar automaticamente sempre que é ligado um dispositivo de armazenamento ao computador e analisá-lo.Utilize esta tarefa para configurar as opções da detecção e análise automática de dispositivos de armazenamento (CDs/DVDs, dispositivos USB ou unidades de rede mapeadas).

Menu Contextual da Análise

Esta tarefa é utilizada na análise a partir do menu de contexto do Windows ou da barra de actividade de análise.Pode modificar as opções de análise consoante as suas necessidades.

Pode gerir as tarefas de análise com os botões ou com o menu de atalho.

Para levar a cabo uma tarefa de análise do sistema ou definida por si, clique no botão **Executar Tarefa** button.O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise.

Para definir a execução automática de uma tarefa de análise, mais tarde ou regularmente, clique no respectivo botão **Agendar** e configure o agendamento da tarefa consoante o necessário.

Se já não precise de uma tarefa de análise que criou, pode pagá-la clicando no botão **Apagar** localizado do lado direito da tarefa.Não pode apagar tarefas de sistema ou variadas.

Cada tarefa de análise possui uma janela de Propriedades, onde pode configurar as definições e ver os relatórios de análise.Para abrir esta janela clique em **Propriedades** localizado no botão do lado esquerdo da tarefa (ou clique com o botão direito do rato na tarefa e depois clique em **Propriedades**).

Para saber mais, consulte os seguintes tópicos:

- “*Configurar Definições da Análise*” (p. 79)
- “*Definir Alvo da Análise*” (p. 82)
- “*Agendar Tarefas de Análise*” (p. 82)

Usando o Menú de Atalho

Um menú de atalho está disponível para cada tarefa. Clique com o botão direito do rato sobre a tarefa para a abrir.

Para as tarefas de sistema ou definidas pelo utilizador, os seguintes comandos estão disponíveis no menu de atalhos:

- **Analisar Agora** - executa a tarefa seleccionada, dando início a uma análise imediata.
- **Caminho** - Abre a janela das **Propriedades**, botão Caminho onde pode modificar o alvo da análise para a tarefa seleccionada.No caso de tarefas do sistema, esta opção é substituida por **Mostrar Caminhos de Análise**, onde apenas poderá ver o alvo da sua análise.
- **Agendar** - abre a janela das **Propriedades** e o botão Agendar, onde pode agendar a tarefa seleccionada.
- **Relatórios** - abre a janela das **Propriedades** e o botão Relatórios onde pode ver os relatórios gerados após as tarefas seleccionadas terem sido executadas.
- **Duplicar Tarefa** - duplica a tarefa seleccionada.Isto é útil na criação de novas tarefas, pois pode modificar as definições da tarefa duplicada.
- **Apagar** - elimina a tarefa seleccionada.

Nota
Disponível apenas para tarefas criadas pelo utilizador. Não pode remover uma tarefa predefinida.

- **Propriedades** - abra a janela **Propriedades**, e o botão Geral , onde pode modificar as configurações para a tarefa seleccionada.

Devido à sua natureza em particular, das **Tarefas Misc** categoria, apenas **Ver Relatório** e **Propriedades** estão disponíveis neste caso.

Configurar Definições da Análise

Para configurar as opções de análise de uma específica tarefa de análise, faça clique-botão direito e seleccione **Propriedades**.

Pode facilmente configurar as opções de análise ajustando o nível de análise. Arraste o cursor ao longo da escala para definir o nível de análise pretendido.Utilize a descrição do lado direito da escala para escolher o nível de análise que melhor se adequa às suas necessidades.

Também pode configurar as seguintes opções gerais:

- **Execute a tarefa de análise com prioridade baixa.** Diminui a prioridade do processo de análise. Irá permitir que outros programas funcionem com maior rapidez e aumenta o tempo necessário para terminar o processo da análise.
- **Minimizar a janela da análise para a área de notificação.** Minimiza a janela da análise no Windows para a área de notificação. Faça duplo-clique sobre o ícone BitDefender para o abrir.
- Especifique a acção a aplicar se não forem encontradas ameaças.

Os utilizadores avançados poderão querer tirar partido das configurações de análise que o BitDefender oferece. O analisador pode ser configurado para evitar extensões de ficheiros, directorias ou arquivos que sabe serem inofensivos. Isto poderá reduzir o tempo de análise e melhorar a resposta do seu computador durante uma análise.

Para configurar em detalhe as definições de análise:

1. Clique em **Personalizar**.
2. Configure as definições de análise como necessário.Para saber o que uma opção faz, mantenha o rato sobre a mesma e leia a descripção apresentada no fundo da janela.
3. Clique em **OK** para guardar as alterações e fechar a janela.

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no glossário.Pode também encontrar informação útil pesquisando a Internet.
- **Nível de Análise.** Especifique que tipo de malware quer que o BitDefender analise seleccionando as opções apropriadas.
- **Análise de ficheiros.** Pode definir o BitDefender para analisar todos os ficheiros acedidos, apenas aplicações (ficheiros de programa) ou tipos de ficheiro específicos que achar perigosos.A análise de todos os ficheiros proporciona uma maior segurança, enquanto a análise das aplicações só pode ser utilizada numa análise mais rápida.

  As aplicações (ou ficheiros de programa) são muito mais vulneráveis a ataques de malware do que qualquer outro tipo de ficheiros.Esta categoria inclui as seguintes extensões de ficheiro:`.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  Se optar por **Analisar extensões definidas pelo utilizador**, é recomendado que inclua todas as extensões de aplicação para além das extensões de ficheiros que considere perigosas.

- **Analisar só ficheiros alterados.** Ao analisar apenas ficheiros novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.
- **Analisar dentro dos arquivos.** Os arquivos que contém ficheiros infectados não são uma ameaça imediata à segurança do seu sistema.O malware só pode afectar o seu sistema se o ficheiro infectado for extraído do arquivo e executado sem que a protecção em tempo real esteja activada.No entanto, é recomendado que utilize esta opção para detectar e remover qualquer ameaça potencial, mesmo se não for imediata.

Nota
Analisar ficheiros arquivados aumenta o tempo da análise e requer mais recursos do sistema.

- **Opções de acção.** Especifique as ações a serem tomadas em cada categoria de ficheiros detectados usando as opções nesta categoria.Há três categorias de ficheiros detectados:
  - **Ficheiros infectados.** Os ficheiros detectados como infectados correspondem a uma assinatura de malware na Base de Dados de Assinaturas de Malware do BitDefender.Por norma, o BitDefender consegue remover o código de malware de um ficheiro infectado e reconstruir o ficheiro original. Esta operação é conhecida por desinfecção.

Nota
As assinaturas de malware são fragmentos de código extraídos de amostras de malware. São utilizados por programas antivírus para efectuar correspondência entre padrões e detectar malware.
A Base de Dados de Assinatura de Malware BitDefender é uma colecção de assinaturas de malware actualizada a toda hora pelos investigadores de malware da BitDefender.

  - **Ficheiros suspeitos.** Os ficheiros são detectados como suspeitos pela análise heurística.Não foi possível desinfectar os ficheiros suspeitos por não estar disponível uma rotina de desinfecção.
  - **Ficheiros ocultos (rootkits).** Repare que este ficheiros ocultos, não são os ficheiros que esconde deliberadamente no Windows. Eles são ficheiros ocultos por programas especiais, conhecidos como rootkits.Os rootkits não são maliciosos por natureza, No entanto, eles são vulgarmente utilizados para tornar os vírus ou o spyware indetectáveis pelos programas antivírus.

Não deve alterar a acções predefinidas aplicadas aos ficheiros detectados excepto se tiver uma forte razão para isso.

Para definir uma nova acção, clique na actual **Primeira acção** e seleccione a opção desejada a partir do menu.Especifique uma **Acção secundária** caso haja falha na principal.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

Definir Alvo da Análise

Não pode modificar os alvos de análise das tarefas de análise a partir da categoria **tarefas do Sistema**.Apenas pode ver o alvo da análise deles.Para ver o alvo da análise de uma determinada tarefa de análise do sistema, faça clique com o botão direito do rato sobre a tarefa e seleccione **Mostrar Caminho da Análise**.

Para definir o alvo da análise de uma determinada tarefa de análise, clique botão direito na tarefa e seleccione **Caminhos**. Alternativamente, se já se encontra na janela das Propriedades da tarefa, seleccione a barra **Caminhos**.

Pode ver a lista das drives locais amovíveis e de rede, como também, se houver, os ficheiros e as pastas adicionada previamente. Todos os items seleccionados serão analisados quando a tarefa for executada.

Estão disponíveis os seguintes botões:

- **Adicionar Itens** - abre uma janela de exploração, onde pode seleccionar o(s) ficheiro(s) e pasta(s), que pretende analisar.

Nota
Use carregar & descarregar para adicionar à lista ficheiros/pastas.

- **Apagar item** - remove o(s) ficheiro (s) / pasta(s) que foram previamente seleccionados da lista dos objectos a serem analisados.

Para além destes botões, existem algumas opções que permitem uma selecção rápida das áreas a analisar.

- **Unidades Locais** - para analisar as drives locais.
- **Unidades de Rede** - para analisar todas as drives de rede.
- **Unidades Amovíveis** - para analisar todas as drives amovíveis (CD-ROM, unidade de disquetes).
- **Todas as Entradas** - para analisar todos as drives, independentemente de serem locais, de rede ou amovíveis.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

Agendar Tarefas de Análise

Com tarefas complexas, o processo de análise leva algum tempo, e funciona melhor se fechar todos os outros programas. É por isso que é melhor agendar tais tarefas

para quando não estiver a utilizar o seu computador e este tenha entrado no modo de descanso.

Para ver o agendamento de uma determinada tarefa ou modificá-lo, clique botão direito do rato e seleccione **Agendar**. Se já se encontra na janela das Propriedades, seleccione a barra **Agendador**.

Se houver, pode ver a tarefa agendada.

Quando agendar uma tarefa, deve de escolher uma das seguintes opções:

- **Não** - executa a tarefa apenas quando o utilizador a solicita.
- **Uma vez** - Executa a análise uma só vez, num determinado momento. Definir a data de início e a hora nos campos**Iniciar Data/Hora**
- **Periodicamente** - Executa a análise periodicamente, num determinado intervalo de tempo (horas, dias, semanas, meses, anos) começando a uma determinada data e hora.
- **No iniciar do sistema** - Executa a análise, após um determinado número de minutos especificados, após o utilizador entrar no Windows.

Clique em **OK** para guardar as alterações e fechar a janela. Para executar a tarefa, apenas clique em **Analisar**.

15.3. Configurar Exclusões da Análise

Há casos em que tem de excluir certos ficheiros de serem analisados. Por exemplo, poderá querer excluir um ficheiro de teste EICAR da análise no acesso ou os ficheiros `.avi` da análise a pedido.

BitDefender permite-lhe excluir objectos da análise no-acesso e da análise a-pedido, ou de ambas. Esta definição tem o propósito de diminuir o tempo de análise e evitar interferência com o seu trabalho.

Dois tipos de objectos podem ser excluidos da análise:

- **Caminhos** - o ficheiro ou pasta (incluindo os objectos que contém) indicados por um determinado caminho serão excluídos da análise.
- **Extensões** - todos os ficheiros com a extensão especificada serão excluídos da análise, independentemente da localização no disco rígido.

Os objectos excluídos da análise a-pedido não serão analisados, independentemente de eles serem acedidos por si ou por uma aplicação.

Nota

As exclusões NÃO serão aplicadas à análise contextual.Análise Contextual é um tipo de análise a-pedido: você clica com o botão direito de rato sobre o ficheiro ou pasta que quer analisar e selecciona **Analisar com BitDefender**.

15.3.1. Excluir Ficheiros ou Pastas da Análise

Para excluir caminhos da análise:

1. Abrir o BitDefender.
2. Dependendo do modo de interface do utilizador, proceda da seguinte forma:

   Modo Intermédio
   : Abra o separador **Segurança** e clique em **Configurar o Antivírus**, nas Tarefas Rápidas, no lado esquerdo da janela.

     Vá ao separador **Exclusões**.

   Modo Avançado
   : Vá a **Antivírus > Exclusões**.

   ### Nota

   No Modo Básico e no Modo Intermédio, pode configurar um atalho para poder aceder a estas definições a partir do painel de instrumentos.Para mais informação, por favor consulte o *“Ferramentas”* (p. 36).

3. Seleccione a respectiva caixa para activar as exclusões de análise.
4. Inicie o assistente de configuração da seguinte forma:
   - Clique com o botão direito na tabela Ficheiros e Pastas e seleccione **Adicionar novo caminho**.
   - Clique no botão **Adicionar**, localizado no cimo da tabela de exclusões.
5. Siga o assistente de configuração.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

   a. Seleccione a opção de excluir um caminho da análise.Este passo só aparece quando inicia o assistente clicando no botão **Adicionar**.

   b. Para especificar os caminhos a excluir da análise use os seguintes métodos:
      - Clique em **Explorar**, seleccione o ficheiro ou pasta que deseja excluir da análise e depois clique **Adicionar**.
      - Insira o caminho que deseja que seja excluído da análise no campo editado e clique em **Adicionar**.

      Os caminhos surgirão na lista à medida que os adicione. Pode adicionar tantos caminhos quanto os que deseje.

   c. Por defeito, os caminhos seleccionados são excluídos da análise no-acesso e a-pedido. Para alterar isto, clique na coluna à direita e seleccione a opção desejada da lista.

d. É altamente recomendável analisar os ficheiros nos caminhos especificados para ter a certeza de que não estão infectados.Seleccione a caixa de selecção para analisar estes ficheiros antes de os excluir da análise.

Clique em **Concluir** para adicionar exclusões da análise.

6. Prima **Aplicar** para guardar as alterações.

15.3.2. Excluir Extensões de Ficheiros da Análise

Para excluir extensões de ficheiro da análise:

1. Abrir o BitDefender.
2. Dependendo do modo de interface do utilizador, proceda da seguinte forma:

Modo Intermédio

Abra o separador **Segurança** e clique em **Configurar o Antivírus**, nas Tarefas Rápidas, no lado esquerdo da janela.

Vá ao separador **Exclusões**.

Modo Avançado

Vá a **Antivírus > Exclusões**.

Nota

No Modo Básico e no Modo Intermédio, pode configurar um atalho para poder aceder a estas definições a partir do painel de instrumentos.Para mais informação, por favor consulte o “*Ferramentas*” (p. 36).

3. Seleccione a respectiva caixa para activar as exclusões de análise.
4. Inicie o assistente de configuração da seguinte forma:

- Clique com o botão direito na tabela de Extensões e seleccione **Adicionar novas extensões**.
- Clique no botão **Adicionar**, localizado no cimo da tabela de exclusões.

5. Siga o assistente de configuração.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

a. Seleccione a opção de excluir extensões da analiseEste passo só aparece quando inicia o assistente clicando no botão **Adicionar**.

b. Para especificar as extensões a serem excluídas da análise use os seguintes métodos:

- Seleccione a partir do menu a extensão que deseja excluir da análise e clique em **Adicionar**.

Nota

O menu contém uma lista de extensões registadas no seu sistema. Quando selecciona uma extensão, pode ver a sua descripção, caso a mesma esteja disponível.

- Insira a extensões que deseja excluir da análise no campo editar e clique em **Adicionar**.

As extensões aparecerão na lista à medida que as adiciona. Pode adicionar tantas extensões quantas as que desejar.

c. Por defeito, as extensões seleccionadas são excluidas da análise no-acesso e a-pedido. Para alterar isto, clique na coluna da direita e seleccione a opção que deseja a partir da lista.

d. É altamente recomendável analisar os ficheiros com as extensões especificadas para ter a certeza de que não estão infectados.

Clique em **Concluir** para adicionar exclusões da análise.

6. Prima **Aplicar** para guardar as alterações.

15.3.3. Gerir Exclusões da Análise

Se as exclusões de análise configuradas já não forem necessárias, é recomendado que elimine ou desactive as exclusões da análise.

Para gerir as exclusões da análise:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Exclusões**.

Para eliminar um item da lista, seleccione-o e clique no botão **Apagar**.

Para editar uma entrada da lista, seleccione-a e clique no botão **Editar**.Aparecerá uma nova janela onde poderá alterar a extensão ou o caminho a ser excluído e o tipo de análise da qual quer que eles sejam excluídos. Faça as alterção necessárias e clique **OK**.

Nota

Pode também clicar no objecto usando o botão direito do rato e utilizar as opções que aparecem no menu de atalho para o editar ou apagar.

Para desactivar exclusões de análise, desmarque a respectiva caixa de selecção.

15.4. Àrea de Quarentena

O BitDefender permite o isolamento de ficheiros infectados ou suspeitos numa área segura, chamada de quarentena. Ao isolar estes ficheiros na quarentena, desaparece

o risco de infecção,e ao mesmo tempo, terá a possibilidade de enviar estes ficheiros para análise no laboratório do BitDefender.

Nota
Quando o vírus se encontra na quarentena não pode provocar nenhum mal, porque não pode ser nem lido nem executado.

Em adição, o BitDefender analisa os ficheiros em quarentena após cada actualização das assinaturas de malware.Os ficheiros limpos são automaticamente repostos no seu local de origem.

Para ver e gerir os ficheiros na quarentena e configurar as definições da quarentena:

1. Abrir o BitDefender.
2. Dependendo do modo de interface do utilizador, proceda da seguinte forma:

   Modo Intermédio
   : Abra o separador **Segurança** e clique em **Configurar o Antivírus**, nas Tarefas Rápidas, no lado esquerdo da janela.

     Abra o separador **Quarentena**.

   Modo Avançado
   : Vá a **Antivírus > Quarentena**.

Nota
No Modo Básico e no Modo Intermédio, pode configurar um atalho para poder aceder a estas definições a partir do painel de instrumentos.Para mais informação, por favor consulte o *"Ferramentas"* (p. 36).

Gerir Ficheiros em Quarentena

Pode enviar qualquer ficheiro seleccionado da quarentena para os Laboratórios BitDefender clicando no botão **Enviar**.Por defeito o BitDefender envia automaticamente os ficheiros em quarentena a cada 60 minutos.

Para eliminar um ficheiro da quarentena, seleccione-o e clique no botão **Eliminar**.

Se pretende restaurar um ficheiro da quarentena para a respectiva localização original, seleccione-o e clique em **Restaurar**.

Configuração da Quarentena

Para configurar as definições da quarentena, clique em **Configuração**.Ao usar a configuração da quarentena, pode definir o BitDefender para executar automaticamente as seguintes acções:

Apagar ficheiros antigos. Para apagar automaticamente ficheiros antigos da quarentena, seleccione a opção correspondente.Deve especificar o número de dias

após os quais os ficheiros em quarentena deverão ser apagados e a frequência com a qual o BitDefender deve de verificar esta situação.

Enviar os ficheiros automaticamente. Para enviar automaticamente ficheiros em quarentena, seleccione a opção correspondente.Deve de especificar a frequência com que deseja enviar os ficheiros.

Analisar os ficheiros em quarentena após a actualização. Para analisar automaticamente ficheiros em quarentena após a actualização, seleccione a opção correspondente.Pode escolher mover automaticamente os ficheiros limpos para a sua localização original seleccionado a opção **Restaurar Ficheiros Limpos**.

Clique em **OK** para guardar as alterações e fechar a janela.

16. Protecção Antiphishing

O BitDefender Antiphishing impede que seja revelada informação pessoal enquanto explora a internet ao alertá-lo acerca das páginas web potencialmente phishing.

O BitDefender dá-lhe uma protecção Antiphishing em tempo-real para:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

16.1. Configurar a Lista Branca de Antiphishing

Pode configurar e gerir uma lista branca de sítios de Internet que não serão analisados pelos motores Antiphishing do BitDefender.A lista branca deve de conter apenas os websites em que confia plenamente.Por exemplo, adicione os websites onde costuma frequentemente fazer compras on-line.

Nota

Pode de forma fácil e eficiente gerir a protecção antiphishing e a Lista Branca usando a barra de ferramentas do BitDefender Antiphishing que está integrada no Internet Explorer.Para mais informação, por favor consulte o *"Gerir a Protecção Antiphishing do BitDefender no Internet Explorer e Firefox"* (p. 89).

Para configurar e gerir a lista branca de antiphishing:

- Se estiver a usar um navegador da Internet compatível, clique na barra de ferramentas do BitDefender e seleccione **Lista Branca** no menu.
- Em alternativa, proceda da seguinte forma:
  1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
  2. Vá a **Antivírus > Escudo**.
  3. Clique em **Lista Branca**.

Para adicionar um site à Lista Branca, insira o seu endereço no campo correspondente e depois clique em **Adicionar**.

Para remover um site web da lista branca, seleccione-a e clique **Remover**.

Clique em **Guardar** para guardar as alterações e fechar a janela.

16.2. Gerir a Protecção Antiphishing do BitDefender no Internet Explorer e Firefox

BitDefender integra-se directamente através de uma barra de tarefas intuitiva e fácil de usar nos seguintes exploradores da Internet:

- Internet Explorer
- Mozilla Firefox

Pode de forma fácil e eficiente gerir a protecção antiphishing e a Lista Branca usando a barra de ferramentas do BitDefender Antiphishing que está integrada num dos exploradores da internet acima.

A barra de ferramentas antiphishing representado pelo ícone do BitDefender , encontra-se no lado superior do Explorador da Internet.Clique nele de forma a abrir o menu da barra de ferramentas.

Nota
Se não consegue ver a barra de ferramentas, abra o menu **Ver** siga para **Barras de ferramentas** e seleccione **Barra de Ferramentas BitDefender**.

Os seguintes comandos estão disponíveis no menu da barra de ferramentas:

- **Activar / Desactivar** - activa / desactiva a barra de ferramentas Antiphishing do BitDefender, no presente explorador de internet.
- **Configuração** - abre uma janela onde pode especificar as definições da barra de ferramentas do antiphishing.Estão disponíveis as seguintes opções:
  - **Protecção Antiphishing Wen em Tempo-real** - detecta e alerta-o em tempo-real se um site web é de phishing (preparado para lhe roubar informação pessoal).Esta opção controla a protecção antiphishing BitDefender apenas no actual explorador da internet.
  - **Avisar antes adicionar à lista branca** - será consultado antes de ser adicionado um site web à Lista Branca.
- **Adicionar à Lista Branca** - adiciona o actual site web à Lista Branca.

Importante
Adicionar um site à Lista Branca significa que o BitDefender não irá mais analisar esse site em busca de tentativas de phishing. Recomendamos que adicione à Lista Branca apenas os sites em que confia totalmente.

- **Lista Branca** - abre a Lista Branca.Para mais informação, por favor consulte o *"Configurar a Lista Branca de Antiphishing"* (p. 89).
- **Relatar como Phishing** - informa o Laboratório BitDefender que você considera determinado site web como sendo usado para phishing.Ao reportat sites de phishing você ajuda a proteger outros contra o roubo de identidade.
- **Ajuda** - abre a documentação electrónica.
- **Acerca** - abre uma janela onde pode ver informação acerca do BitDefender e onde procurar ajuda caso algo de inesperado lhe apareça.

17. Consultor de Procura

O Consultor de Procura melhora a protecção contra ameaças em linha alertando sobre páginas da Internet de phishing ou inseguras directamente na página com os resultados das suas pesquisas.

O Consultor de Procura é compatível com todos os navegadores de Internet e analisa os resultados da pesquisa apresentados pelos motores de busca mais conhecidos:

- Google
- Yahoo!
- Bing

O Consultor de Procura indica se um resultado da pesquisa é seguro ou não, colocando um pequeno ícone de estado antes da hiperligação.

Círculo verde com uma marca de verificação: Pode aceder com segurança à hiperligação.

Circulo vermelho com um ponto de exclamação: Esta é uma página de Internet de phishing ou que não é de confiança.Deve evitar abrir esta hiperligação.Se estiver a utilizar o Internet Explorer ou o Firefox e tentar abrir a hiperligação, o BitDefender irá bloquear automaticamente a página de Internet e apresentar antes uma página de alerta.Se pretende ignorar o alerta e aceder à página de Internet, siga as instruções na página de alerta.

17.1. Desactivar o Consultor de Procura:

Para desactivar o Consultor de Procura:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Preferências**.
2. Vá a **Definições de Segurança**.
3. Utilize o botão para desactivar o Consultor de Procura.

18. Antispam

Spam é o termo utilizado para descrever mensagens electrónicas não solicitadas.O Spam é um problema crescente, tanto para indíviduos como para organizações. Não é bonito, não desejaria que os seus filhos o vissem, pode fazer com que seja despedido (por desperdiçar muito tempo, ou por receber pornografia no seu mail de trabalho) e pode impedir que as pessoas o enviem. O melhor a fazer para impedir isso, é, obviamente, parar de o receber. Infelizmente, o Spam num largo domínio de formas e tamanhos, e é muito existente.

O BitDefender Antispam emprega inovações tecnológicas surpreendentes e um conjunto de filtros de antispam standard para limpar o spam antes de o mesmo chegar à caixa de correio A receber do utilizador.Para mais informação, por favor consulte o “*Compreender o Antispam*” (p. 92).

A protecção de Antispam do BitDefender está disponível apenas para clientes de correio electrónico configurado para receber mensagens de e-mail via protocolo POP3.POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio.

Nota
O BitDefender não proporciona protecção antispam para contas de correio electrónico a que acede através de sítios de Internet (webmail).

As mensagens não solicitadas detectadas pelo BitDefender são marcadas com o prefixo `[SPAM]` no campo do assunto.O BitDefender move automaticamente as mensagens de spam para uma determinada pasta, da seguinte forma:

- No Microsoft Outlook, as mensagens de spam são movidas para a pasta **Spam**, localizada na pasta **Itens Eliminados**.A pasta **Spam** é criada durante a instalação do BitDefender.
- No Outlook Express e no Windows Mail, as mensagens de spam são movidas directamente para os **Itens Eliminados**.
- No Mozilla Thunderbird, as mensagens de spam são movidas para a pasta **Spam**, localizada na pasta **Lixo**.A pasta **Spam** é criada durante a instalação do BitDefender.

Se utilizar outros clientes de correio electrónico, deve criar uma regra para mover as mensagens electrónicas marcadas como `[spam]` pelo BitDefender para uma pasta de quarentena personalizada.

18.1. Compreender o Antispam

18.1.1. Filtros Antispam

O Motor Antispam do BitDefender Antispam incorpora sete filtros distintos, os quais asseguram que a sua Caixa de Entrada de correio se mantenha livre de SPAM: Lista

Amigos, Lista Spammers, Filtro caracteres, Filtro de Imagem, Filtro URL, Filtro NeuNet (Heurístico) e Filtro Bayesiano.

Lista de Spammers / Amigos

A maioria das pessoas comunica regularmente com um grupo de pessoas, ou até mesmo recebe mensagens de empresas ou organizações no mesmo domínio. Ao utilizar as **listas de amigos ou spammers**, pode facilmente decidir de quem pretende receber e-mails (amigos) independentemente do conteúdo das mensagens, ou de quem nem sequer pretende ouvir falar novamente (spammers).

Nota

Recomendamos que adicone os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O BitDefender não bloqueia mensagens dos presentes nessa lista; deste modo, a adição de amigos ajuda a assegurar a passagem de mensagens legítimas.

Filtro de caracteres

A maioria das mensagens de spam estão escritas em caracteres Cirílicos ou Asiáticos. O filtro de Caracteres detecta este tipo de mensagens e marca-os como SPAM.

Filtro de Imagem

Uma vez que evitar o filtro heurístico se tornou um desafio e tanto, hoje em dia as pastas de entrada dos e-mails estão cada vez mais cheias de mensagens contendo apenas uma imagem com conteúdo não-solicitado. Para fazer face a este problema crescente, BitDefender introduziu o **Filtro de Imagem** que compara a assinatura do e-mail com aquelas da base de dados do BitDefender. Em caso de igualdade o e-mail será etiquetado com SPAM.

Filtro URL

A maioria das mensagens de Spam contém links para vários locais da web. Estes locais por sua vez contém mais publicidade e a possibilidade de comprar coisas, e por vezes, são usados para phishing.

O BitDefender mantém uma base de dados de tais links.O filtro URL verificas cada link URL numa mensagem e compara-o com a sua base de dados. Se existir uma correspondência, a mensagem é marcada como SPAM.

Filtro NeuNet (Heurístico)

O **Filtro NeuNet (Heurístico)** executa uma série de testes nos componentes da mensagem (por ex., não só o cabeçalho mas também todo o corpo da mensagem, seja em formato HTML ou em texto), procurando palavras, frases, links ou outras características de SPAM.Baseado nos resultados da análise, adiciona uma marca de SPAM à mensagem.

O filtro também detecta mensagens marcadas como SEXUALMENTE EXPLÍCITO: no assunto e marca-as como SPAM.

Nota

Desde 19 de Maio de 2004, o Spam com conteúdo de caracter sexual, tem de incluir o aviso SEXUALMENTE EXPLÍCITO: no assunto ou está sujeito a multa por violação da lei.

Filtro Bayesiano

O modulo do **Filtro Bayesian** classifica as mensagens de acordo com as informações estatísticas, tendo em conta a taxa de palavras específicas que aparecem nas mensagens classificadas como Indesejadas, comparadas com aquelas que não são Indesejadas (por si ou pelo filtro heurístico).

Isto significa, por exemplo, se uma certa carta de quatro palavras aparece mais frequentemente como Indesejada, é natural que assuma que existe uma maior possibilidade de a próxima mensagem que a inclua, seja vista como Indesejada. Todas as palavras relevantes, dentro de uma mensagem, são levadas em conta. Ao sintetizar a informação estatística, é computizada a maior probabilidade de toda a mensagem ser Indesejada.

Este modulo apresenta outra característica interessante: é treinável. Adapta-se rapidamente ao tipo de mensagens recebidas por um dado utilizador, e armazena informação acerca de todos. Para funcionar com eficiência, o filtro tem de ser treinado, o que significa, apresentar-lhe amostras de Spam e de mensagens legítimas, tal como um predador é impelido de caçar uma certa presa. Ás vezes o filtro também tem de ser corrigido – pronto a ajustar-se quando toma uma decisão errada.

Importante

Pode corrigir o módulo Bayesiano ao usar os botões **É Spam** e **Não é Spam** da Barra de tarefas Antispam.

18.1.2. Operação Antispam

O Motor BitDefender Antispam usa todos os filtros antispam combinados para determinar se um determinado e-mail deve de chegar à pasta **A Receber** ou não.

Todo o e-mail proveniente da Internet é inicialmente verificado pelo filtro da Lista Amigos / Lista Spammers. Se o endereço do remetente se encontrar na Lista Amigos, o e-mail é movido directamente para a sua **Caixa de Entrada**.

Caso contrário, o filtro da Lista de Spammers irá apoderar-se do seu correio electrónico para verificar se o endereço do remetente se encontra na lista. Se for encontrada uma correspondência, a mensagem será marcada como SPAM e movida para a pasta de **Spam**.

Ainda, o Filtro caracteres irá verificar se o e-mail está escrito em caracteres Cirílicos ou Asiáticos. Se assim for, e-mail será marcado com Indesejado e movido para a pasta de **Spam**.

Se o e-mail não estiver escrito em caracteres Cirílicos ou Asiáticos, irá passar pelo Filtro de Imagem. O **Filtro de Imagem** detecta todas as mensagens de e-mail que contêm imagens anexadas com conteúdo de spam.

O Filtro de URL vai comparar as hiperligações encontradas na mensagem electrónica com as hiperligações existentes na base de dados de spam do BitDefender. Se houver correspondência, a mensagem electrónica será classificada como SPAM.

O Filtro NeuNet (Heurístico) irá apoderar-se do e-correio electrónico e irá executar uma série de testes aos componentes da mensagem, procurando palavras, frases, hiperligações e outras características de SPAM.Com base nos resultados da análise, o correio electrónico receberá uma pontuação de spam.

Nota

Se o e-mail for marcado com SEXUALLY EXPLICIT na linha do sujeito, o BitDefender irá considerá-lo como SPAM.

O modulo do Filtro Bayesian irá seguidamente analisar a mensagem, de acordo com as informações estatísticas, tendo em conta a taxa de palavras específicas que aparecem nas mensagens classificadas como Indesejadas, comparadas com aquelas que não são Indesejadas (por si ou pelo filtro heurístico). Irá ser adicionada à mensagem uma marca de Spam.

Se a pontuação geral de spam (pontuação heurística + pontuação bayesiana) exceder o limite, a mensagem electrónica é considerada como SPAM.O nível limite é definido pelo nível de protecção antispam.Para mais informação, por favor consulte o *"Ajustar o Nível de Protecção"* (p. 101).

18.1.3. Actualização do Antispam

Cada vez que executa uma actualização:

- novas assinaturas de imagens serão adicionadas ao **Filtro de Imagem**.
- novos links serão adicionados ao **Filtro de URL**.
- novas regras serão adicionadas ao **filtro NeuNet (Heurístico)**.

Isto ajuda a umentar a eficiência da engenharia Antispam.

Para o proteger contra os spammers, BitDefender pode levar a cabo actualizações automáticas. Mantenha a opção **Actualização Automática** active.

18.2. Assistente de Optimização Antispam

A primeira vez que executar o seu cliente de e-mail, um assistente irá aparecer para o ajudar a configurar a Lista de Amigos e a Lista de Spammers e a treinar o Filtro Bayesiano, para aumentar a eficiência dos filtros Antispam.

Nota
O assistente pode ser executado a qualquer altura que deseje clicando no botão **Assistente** na Brra de tarefas Antispam.

Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Se quiser passar um passo de configuração, seleccione **Saltar este passo**.Para sair do assistente, clique em **Cancelar**.

1. **Janela de boas-vindas**
2. **Adicionar os Contactos à Lista de Amigos**

   Aqui pode ver todos os endereços do seu **Livro de Endereços**. Por favor seleccione os que pretende adicionar à sua **Lista de Amigos** (recomendamos que seleccione todos). Irá receber todas as mensagens de e-mail desses endereços, independentemente do seu conteúdo.

   Para adicionar todos os seus contactos à lista de Amigos, seleccione **Seleccionar todos**.

3. **Apagar a Base de Dados Bayesiana**

   Nota
   Na primeira vez que executa o assistente, avance para o passo seguinte.

   Poderá achar que o filtro de Antispam começou a perder eficiência. Isto pode estar relacionado com o treino impróprio (por ex. por erro, marcou um número de mensagens legítimas como Indesejadas, ou vice versa). Se o seu filtro for pouco impreciso, poderá necessitar de limpar a base de dados e voltar a treinar o filtro ao seguir os passos do assistente.

   Seleccione **Limpar dados do filtro Antispam** se pretende efectuar uma nova composição da base de dados do filtro Bayesian.

   Pode guardar a base de dados Bayesiana num ficheiro para que o possa utilizar com outros produtos BitDefender ou após reinstalar o BitDefender.Para guardar a base de dados Bayesiana, clique no botão **Guardar Bayes** e guarde no local desejado.o ficheiro terá a extensão `.dat`.

   Para carregar uma base de dados Bayesiana anterior, clique no botão **Carregar Bayes** e abra o ficheiro correspondente.

4. **Treinar o filtro Bayesian com mensagens electrónicas legítimas (não spam)**

Por favor seleccione a pasta que contém mensagens de e-mail legítimas. Estas mensagens serão usadas para treinar o filtro Bayesian.

existem duas opções avançadas por debaixo da lista de directórios:

- **Incluir sub-pastas** - para adicionar as sub-pastas à sua selecção.
- **Adicionar automaticamente à lista de Amigos** - para adicionar os remetentes à lista de Amigos.

5. **Treinar o Filtro Bayesiano com Mensagens Indesejadas**

Por favor seleccione a pasta que contém mensagens de e-mail indesejadas. Estas mensagens serão usadas para treinar o filtro Bayesian.

Importante

Por favor certifique-se que a pasta que escolher não contém, de modo, algum, me-mails legítimos; de outro modo, o desempenho do Antispam será consideravelmente reduzido.

existem duas opções avançadas por debaixo da lista de directórios:

- **Incluir sub-pastas** - para adicionar as sub-pastas à sua selecção.
- **Adicionar automaticamente à lista de Spammers** - para adicionar os remetentes à lista de Spammers.As mensagens de E-mail destes remetentes irão aparecer sempre marcados como SPAM e serão processadas como tal.

6. **Sumário**

Nesta janela pode visualizar todas as definições do assistente de configuração, podendo efectuar alterações, ao retornar aos passos anteriores (clique em **Atrás**).

Se não deseja fazer quaisquer modificações, prima **Terminar** para finalizar o wizard.

18.3. Utilizar a Barra de Ferramentas Antispam na Janela do Seu Cliente de Correio Electrónico

No lado superior da janela do seu cliente de mail pode ver a barra de ferramentas do Antispam.A barra de ferramentas do Antispam ajuda-o a gerir a protecção antispam directamente do seu cliente de e-mail.Pode facilmente corrigir o BitDefender se ele marcar uma mensagem legítima como SPAM.

Importante

O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns.Para ver a lista completa de clientes de e-mail suportados, por favor consulte o “*Requisitos de Software*” (p. 2).

Cada botão é explicado abaixo:

- **É Spam** - envia uma mensagem ao módulo Bayesiano, indicando que o e-mail seleccionado é spam. O e-mail será marcado como SPAM e será movido para a pasta de **Spam**.

  Futuras mensagens que se enquadem nas mesmas patentes serão marcadas como INDESEJADAS.

- **Não é Spam** - envia uma mensagem ao módulo Bayesiano, indicando que o e-mail seleccionado não é spam, e que o BitDefender não o deve marcar como tal.Este e-mail será movido da pasta **Spam** para o directório **Caixa de Entrada**.

  Futuras mensagens que se enquadem nas mesmas patentes já não serão marcadas como INDESEJADAS.

Importante

O botão **Não é Spam** fica activo quando seleccionar uma mensagem marcada como SPAM pelo BitDefender (normalmente estas mensagens localizam-se na pasta de **Spam**).

- **Adicionar Spammer** - adiciona o remetente da mensagem de e-mail à lista de Spammers.Pode necessitar de clicar em **OK** para confirmar.As mensagens de e-mail recebidas dos endereços na lista de Spammers são automaticamente marcadas como `[spam]`.
- **Adicionar Amigo** - adiciona o remetente da mensagem de e-mail à lista de Amigos.Pode necessitar de clicar em **OK** para confirmar.Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.
- **Spammers**- abre a **Lista de Spammers** que contém todos os endereços de e-mail, dos quais não quer receber mensagens, independentemente do seu conteúdo.Para mais informação, por favor consulte o “*Configurar a lista de Spammers*” (p. 102).
- **Amigos** - abre a **Lista de amigos** que contém todos os endereços de e-mail dos quais deseja receber mensagens de e-mail, independentemente do seu conteúdo.Para mais informação, por favor consulte o “*Configurar a Lista de Amigos*” (p. 101).
- **Configuração** - abre a janela das **Configurações** onde pode definir algumas opções para o módulo **Antispam**.
- **Assistente** - abre o assistente de optimização antispam.Este assistente ajuda-o a treinar o Filtro bayesiano para aumentar a eficácia da sua protecção antispam.Também pode adicionar endereços do seu Livro de Endereços à sua Lista de Amigos / Lista de Spammers.
- **Antispam BitDefender** - abre uma janela onde pode configurar o nível de protecção antispam e os filtros antispam.

18.3.1. Indicar os Erros de Detecção

Se estiver a usar um cliente de e-mail suportado, pode facilmente corrigir o filtro antispam (indicando mensagens de correio electrónico que não deveriam ter sido marcadas como`[spam]`). Se o fizer, irá melhorar consideravelmente a eficiência do filtro antispam.Siga estes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo electrónico, para onde são movidas as mensagens.
3. Seleccione a mensagem legítima incorrectamente marcada como `[spam]` pelo BitDefender.
4. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do BitDefender para adicionar o remetente à lista de Amigos.Pode necessitar de clicar em **OK** para confirmar.Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.
5. Clique no botão **Não é Spam** na barra de antispam BitDefender (normalmente localizada na parte superior da janela do cliente de e-mail). Isto indica ao Mecanismo de Aprendizagem que a mensagem seleccionada não é spam. A mensagem de e-mail será movida para a pasta Recebidos.Os próximos e-mails que se encaixem nos mesmos padrões, não serão marcadas como `[spam]`.

18.3.2. Indicar Mensagens de Spam Não Detectadas

Se estiver a utilizar um cliente de e-mail suportado, pode facilmente indicar quais as mensagens de e-mail que devem ser detectadas como spam. Ao fazê-lo melhora, em muito, a eficiência do filtro de antispam.Siga estes passos:

1. Abra o mail de cliente.
2. Vá à pasta Caixa de Entrada.
3. Seleccione as mensagens spam não detectadas
4. Clique no botão **É Spam** na barra de tarefas do BitDefender (normalmente localizada na parte superior da janela de cliente de mail). Isto indica ao Motor de Aprendizagem que as mensagens seleccionadas são spam. São imediatamente marcadas como `[spam]` e movidas para a pasta de lixo electrónico.Os próximos e-mails que se encaixem nos mesmos padrões, serão marcadas como `[spam]`.

18.3.3. Retreinar o Motor de Aprendizagem (Bayesiano)

Se o seu filtro antispam não for exacto, poderá ter de limpar a base de dados bayesiana e retreinar o Filtro Bayesian.

Antes de iniciar o treino do Motor de Aprendizagem (Bayesiano), prepare uma pasta que contenha apenas mensagens SPAM e outra que contenha apenas mensagens legitimas.O Motor de Aprendizagem irá analisá-los e aprender as características

que o definem como spam ou legitimar mensagens que normalmente recebe. Para que a formação seja eficaz, tem de haver mais de 50 mensagens em cada categoria.

Para redefinir a base de dados Bayesiana e retreinar o Motor de Aprendizagem, siga os seguintes passos:

1. Abra o mail de cliente.
2. Na barra de ferramentas antispam do BitDefender, clique no botão **Assistente** para iniciar o assistente de configuração do antispam.
3. Clique **Seguinte**.
4. Seleccione **Saltar este passo** e clique em **Seguinte**.
5. Seleccione **Limpar dados do filtro antispam** e clique **Seguinte**.
6. Seleccione a pasta que contém as mensagens legítimas e clique em **Seguinte**.
7. Seleccione a pasta que contém as mensagens SPAM e clique em **Seguinte**.
8. Clique em **Terminar** para dar início ao processo de treino.
9. Quando o treino está completo, clique em **Fechar**.

18.3.4. Guardar e Carregar a Base de Dados Bayesiana

Pode guardar a base de dados Bayesiana num ficheiro para que o possa utilizar com outros produtos BitDefender ou após reinstalar o BitDefender.

Clique no botão **Definições** da barra de tarefas antispam do BitDefender.

Para guardar a base de dados Bayesiana, clique no botão **Guardar Bayes** e guarde no local desejado.o ficheiro terá a extensão `.dat`.

Para carregar uma base de dados Bayesiana anterior, clique no botão **Carregar Bayes** e abra o ficheiro correspondente.

18.3.5. Configurações Gerais

Para configurar as definições gerais do antispam para o seu cliente de correio electrónico, clique no botão **Definições** na barra de ferramentas antispam do BitDefender.

Estão disponíveis as seguintes opções:

- **Mover mensagens para Itens eliminados** - para mover as mensagens de spam para os **Itens eliminados** (apenas para o Microsoft Outlook Express / Windows Mail);
- **Marcar mensagem como 'Lida'** - para marcar todas as mensagens Indesejadas como lidas, para que, quando chegarem novas mensagens Indesejadas não seja perturbado.

Clique na barra **Alertas** se deseja aceder à secção onde poderá desactivar a aparição da janela de confirmação para os botões **Adicionar Spammer** e **Adicionar Amigo**.

Na janela de **Alertas** pode activar/desactivar a aparição do alerta **Por favor seleccione um e-email** . Este alerta surge quando selecciona um grupo em vez uma mensagem de e-mail.

18.4. Ajustar o Nível de Protecção

Alguns filtros antispam podem identificar mensagens não solicitadas directamente, enquanto outros atribuem uma pontuação de spam à mensagem, com base nas características de spam detectadas.

O nível de protecção antispam é utilizado para determinar se uma mensagem electrónica pode ser considerada spam com base na pontuação total de spam (recebida após a verificação efectuada por todos os filtros antispam).

Não deve alterar o nível de protecção antispam, excepto se a protecção não funcionar como o esperado.No entanto, antes de alterar o nível de protecção, é recomendado que leia *"O Filtro Antispam Não Está a Funcionar Correctamente"* (p. 235) e siga as instruções para corrigir o problema.

Para ajustar o nível de protecção antispam:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antispam > Estado**.
3. Arraste o cursor pela escala para definir o nível de protecção apropriada.Para definir o nível de protecção por defeito (**Moderado a Agressivo**) clique em **Nível por Defeito**.

Utilize a descrição do lado direito da escala para escolher o nível de protecção que melhor se adequa às suas necessidades de segurança.A descrição também informa sobre as acções adicionais que deverá aplicar para evitar possíveis problemas ou para aumentar a eficácia da detecção antispam.

18.5. Configurar a Lista de Amigos

A **Lista de amigos** é uma lista de todos os endereços de e-mail, dos quais deseja sempre receber mensagens, independentemente do seu conteúdo. A mensagens dos seus amigos não serão vistas como Indesejadas, mesmo que contenham Spam.

Nota

Qualquer mail proveniente de um endereço presente na **Lista de amigos**, será automaticamente entregue na sua Caixa de Entrada, sem mais demora.

Para configurar e gerir a lista de Amigos:

- Se estiver a utilizar o Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, clique no botão **Amigos** na barra de ferramentas antispam do BitDefender integrado no seu cliente de correio electrónico.
- Em alternativa, proceda da seguinte forma:
  1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
  2. Vá a **Antispam > Estado**.
  3. Clique em **Gerir Amigos**.

Para adicionar um endereço electrónico, seleccione a opção **Endereço electrónico**, introduza o endereço clique no botão junto ao campo de edição.Sintaxe: nome@dominio.com.

Para adicionar os endereços electrónicos de um domínio específico, seleccione a opção **Nome do domínio**, insira o nome do domínio e clique no botão junto ao campo de edição.Sintaxe:

- @dominio.com, *dominio.com e dominio.com - todos os mails provenientes de dominio.com chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- *dominio* - todos os mails provenientes de dominio (sem interessar os sufixos do dominio) chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- *com - todos os mails que têm este sufixo de domínio com chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo.

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações.Por exemplo, pode adicionar o domínio do endereço electrónico da empresa para a qual trabalha ou de parceiros de confiança.

Para remover um ítem da lista, seleccione-o e clique em **Remover**.Para apagar todos os eventos da lista clique em **Limpar Relatório** e depois **Sim** para confirmar a sua escolha.

Pode guardar a lista de Amigos num ficheiro para que mais tarde possa usá-lo noutro computador ou quando reinstalar o produto.Para guarda a lista de Amigos, clique no botão **Guardar** e guarda no local desejado.O ficheiro terá a extensão `.bwl`

Para carregar uma lista de Amigos previamente guardada, clique no botão **Carregar** e abra o ficheiro `.bwl` correspondente.Para fazer reset ao conteúdo da lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Clique **Aplicar** e **OK** para guardar e fechar a **Lista de amigos**.

18.6. Configurar a lista de Spammers

A **Lista de indesejados** é uma lista de todos os endereços de e-mail, dos quais nunca pretende receber mensagens, independentemente do seu conteúdo.Todo o

mail proveniente de um endereço presente na **Lista de indesejados**, será marcado automaticamente com indesejado, sem mais demora.

Para configurar e gerir a lista de Spammers:

- Se estiver a utilizar o Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, clique no botão **Spammers** na barra de ferramentas antispam do BitDefender integrado no seu cliente de correio electrónico.
- Em alternativa, proceda da seguinte forma:
  1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
  2. Vá a **Antispam > Estado**.
  3. Clique em **Gerir Spammers**.

Para adicionar um endereço electrónico, seleccione a opção **Endereço electrónico**, introduza o endereço clique no botão junto ao campo de edição.Sintaxe: nome@dominio.com.

Para adicionar os endereços electrónicos de um domínio específico, seleccione a opção **Nome do domínio**, insira o nome do domínio e clique no botão junto ao campo de edição.Sintaxe:

- @dominio.com, *dominio.com e dominio.com - todos os mails provenientes de dominio.com serão marcados como INDESEJADOS;
- *dominio* - todos os mails provenientes de dominio (independentemente dos sufixos de domínio) serão marcados como INDESEJADOS;
- *com - todos os mails tendo o sufixo de domínio com serão marcados como INDESEJADOS.

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações.

Atenção

Não adicione domínios de serviços web-mail (tais como o Yahoo, Gmail, Hotmail ou outro) à lista de Spammers. Caso contrário, as mensagens de email recebidas de algum utilizador registado nesses serviços será detectado como spam.Se, por exemplo, adicionar `yahoo.com` à lista de Spammer, todos as mensagens de e-mais recebidas do endereço `yahoo.com`, serão marcadas como `[spam]`.

Para remover um ítem da lista, seleccione-o e clique em **Remover**.Para apagar todos os eventos da lista clique em **Limpar Relatório** e depois **Sim** para confirmar a sua escolha.

Pode guardar a lista de Spam num ficheiro para que mais tarde possa usá-lo noutro computador ou quando reinstalar o produto.Para guarda a lista de Spam, clique no botão **Guardar** e guarda no local desejado.O ficheiro terá a extensão `.bwl`

Para carregar uma lista de spammers previamente guardada, clique no botão **Carregar** e abra o ficheiro `.bwl` correspondente.Para fazer reset ao conteúdo da

lista actual quando carrega uma lista guardada previamente seleccione **Quando carregar, limpar lista actual**.

Clique **Aplicar** e **OK** para guardar e fechar a **Lista de indesejados**.

18.7. Configurar os Filtros e as Definições do Antispam

Como descrito em *“Compreender o Antispam”* (p. 92), o BitDefender utiliza um conjunto de diferentes filtros antspam para identificar o spam.Os filtros antispam são pré-configurados para uma protecção eficaz.

Pode desactivar cada um destes filtros ou alterar as respectivas definições, mas isto não é recomendado.Estas são algumas alterações que poderá querer fazer:

- Dependendo se recebe ou não mensagens electrónicas fiáveis ou não escrita com caracteres asiáticos ou cirílicos, desactive ou active a definição que bloqueia automaticamente estas mensagens.

Nota

A respectiva definição está desactivada nas versões localizadas do programa que utilizam conjuntos de caracteres (por exemplo, na versão russa ou chinesa).

- Se não pretende adicionar automaticamente os destinatários das suas mensagens electrónicas à lista de Amigos, pode desactivar a respectiva definição.Neste caso, pode adicionar os seus contactos à lista de Amigos, como descrito em *“Configurar a Lista de Amigos”* (p. 101).
- Os utilizadores avançados podem tentar ajustar o tamanho do dicionário Bayesiano para obter um melhor desempenho antispam.Um número mais pequenos de palavras vai resultar num processamento antispam mais rápido mas menos exacto.Um maior número de palavras aumentará a precisão da detecção antispam mas demorará mais tempo a aceder ao seu correio electrónico.

Nota

Poderá ser necessário fazer vários ajustes ao tamanho do dicionário Bayesiano para atingir o nível de desempenho desejado.Se o resultado não for o esperado, restaure o tamanho predefinido e recomendado de 200,000 palavras.

Para configurar as definições e os filtros do antispam:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antispam > Definições**.
3. Configure as definições como necessário.Para saber o que uma opção faz, mantenha o rato sobre a mesma e leia a descripção apresentada no fundo da janela.

4. Prima **Aplicar** para guardar as alterações.

Para aplicar as configurações por defeito, clique em **Por Defeito**.

19. Controlo Parental

O Controlo Parental BitDefender permite-lhe controlar o acesso à Internet e a determinadas aplicações para cada conta de utilizador no sistema.

Pode configurar o Controlo Parental para bloquear:

- Páginas web inapropriadas.
- ligação à Internet, durante determinados períodos de tempo (tal como o período de estudo).
- páginas web, mensagens de e-mail e mensagens instântaneas que contenham determinadas palavras-chave.
- aplicações tais como: jogos, programas de partilha de ficheiros e outros.
- mensagens instântaneas enviadas por contacto IM para além dos que estão permitidos.

Importante

Apenas os utilizadores com direitos de administrador no sistema podem aceder e configurar o Controlo Parental.Para ter a certeza de que só você pode modificar as definições do Controlo Parental para qualquer utilizador, pode protegê-las com uma palavra-passe.Ser-lhe-á pedida a palavra-passe cada vez que activar o Controlo Parental para um determinado utilizador.

Assim que configurar o Controlo Parental, poderá facilmente saber o que os seus filhos estão a fazer no computador.

Mesmo quando não está em casa, pode ver as actividades dos seus filhos e alterar as definições do Controlo Parental através do Controlo Parental Remoto.

19.1. Configurar Controlo Parental

Antes de configurar o Controlo Parental, crie contas de utilizador do Windows separadas para os seus filhos. Isto permitir-lhe-á saber o que cada um faz no computador. Deve criar contas de utilizador limitadas (padrão) para que não possam alterar as definições do Controlo Parental.Para mais informação, por favor consulte o *“Como Posso Criar Contas de Utilizador do Windows?”* (p. 218).

Se os seus filhos puderem aceder a uma conta de administrador no computador, tem de definir uma palavra-passe para proteger as definições do Controlo Parental.Para mais informação, por favor consulte o *“Proteger as Definições do Controlo Parental”* (p. 108).

Para Configurar o Controlo Parental

1. Certifique-se que tem a sessão iniciada com a conta de administrador.Apenas os utilizadores com direitos de administrador no sistema podem aceder e configurar o Controlo Parental.
2. Abrir o BitDefender.
3. Consoante o modo do interface de utilizador, aceda ao Controlo Parental da seguinte forma:

   Modo Intermédio
      Abra o separador **Segurança** e clique em **Controlo Parental**, nas Tarefas Rápidas, no lado esquerdo da janela.

   Modo Avançado
      Clique em **Controlo Parental** no menu do lado esquerdo.

Nota

No Modo Básico e no Modo Intermédio, pode configurar um atalho para poder aceder a estas definições a partir do painel de instrumentos.Para mais informação, por favor consulte o “*Ferramentas*” (p. 36).

Pode ver informação sobre o estado do Controlo Parental para cada utilizador de contas do Windows.A faixa etária é listada abaixo de cada nome do utilizador se o Controlo Parental estiver ativado.Se o Controlo Parental estiver desactivado, o estado é **não configurado**.

Para configurar o Controlo Parental para uma determinada conta de utilizador:

1. Utilize o botão para activar o Controlo Parental para essa conta de utilizador.
2. Será pedido que defina a palavra-passe do Controlo Parental.Definir palavra-passe para proteger as Definições do Controlo Parental.Para mais informação, por favor consulte o “*Proteger as Definições do Controlo Parental*” (p. 108).
3. Insira a categoria da faixa etária para permitir que a sua criança acesse aos sites apropriados para a sua idade.A definição da idade da criança vai carregar automaticamente as definições consideradas adequadas para essa classe etária, com base nos padrões de desenvolvimento infantil.
4. Se quiser configurar em detalhe as definições do Controlo Parental, clique em **Definições**.Clique num separador para configurar as características do Controlo Parental:
   - **Controlo Web** - para filtrar a navegação na Internet de acordo com as regras definidas por si na secção Web .
   - **Controlo de Aplicações** - para bloquear o acesso às aplicações no seu computador de acordo com as regras definidas por si na secçãoAplicações.

- **Filtragem Palavra-chave** - para filtrar o acesso à web, ao correio electrónico e às mensagens instântaneas de acordo com as regras definidas por si na secçãoPalavra-chave .
- **Mensagens Instantâneas** - permitir ou bloquear conversas com contactos de acordo com as regras definidas por si na secção Mensagens Instantâneas.

Configure as opções de monitorização consoante o necessário:

- **Envie-me um relatório de actividade para o e-mail.** Sempre que o Controlo Pearental do BitDefender bloqueia uma actividade no utilizador, é enviada uma notificação de e-mail.Tem de configurar primeiro as definições de notificação.
- **Guardar registo de tráfego de internet.** Regista os sites visitados pelo utilizador para os quais o Controlo Parental está activado.

Para mais informação, por favor consulte o “*Monotorizar Actividade das Crianças*” (p. 115).

Se pretende monitorizar e controlar as actividades dos seus filhos no computador e na Internet à distância, active o Controlo Parental Remoto com o botão.Para mais informação, por favor consulte o “*Controlo Parental Remoto*” (p. 118).

19.1.1. Proteger as Definições do Controlo Parental

Se não for a única pessoa com direitos administrativos a utilizar este computador, recomendamos que protega as suas configurações do Controlo Parental com uma palavra-passe.Ao definir uma palavra-passe, irá prevenir que outros utilizadores com direitos administrativos possam mudar as suas definições do Controlo Parental que configurou para um determinado utilizador.

BitDefender irá solicitar-lhe por defeito que defina uma palavra-passe quando activar o Controlo Parental.Para definir protecção por palavra-passe, faça o seguinte:

1. Digite a palavra-passe na campo **Palavra-passe** .
2. Insira de novo a palavra-passe no campo **Reinserir Palavra-passe** para a confirmar.
3. Clique em **OK** para guardar a palavra-passe e fechar a janela.

Uma vez definida a palavra-passe, se desejar modificar as definições do Controlo Parental, ser-lhe-á pedido que insira a palavra-passe.Os outros administradores de sistema (se existirem) terão também de inserir a palavra-passe de forma a poderem alterar as definições do Controlo Parental.

Nota
A palavra-passe não protege quaisquer outras definições do BitDefender.

Caso não defina uma palavra-passe e não queira que a janela para o efeito lhe surja novamente, seleccione **Não solicitar palavra-passe quando activar Controlo Parental**.

Importante

Se esquecer a palavra-passe, terá de reinstalar o programa ou contactar o apoio do BitDefender.

Para remover a protecção por palavra-passe:

1. Abra o BitDefender e clique em **Opções** que se encontra no canto superior direito da janela.
2. Vá a **Definições Gerais**.
3. Utilize o botão para desactivar a opção **Palavra-passe de definições**.
4. Introduza a palavra-passe.
5. Clique em **OK**.

19.1.2. Controlo Web

O **Controlo Web** ajuda-o a bloquear o acesso a web sites com conteúdo inapropriado. Uma lista de candidatos a serem bloqueados, quer sites quer partes dos mesmos, é fornecida e actualizada pelo BitDefender, como parte do processo normal de actualização.

Nota

Quando activa o Controlo Parental e define a idade do seu filho, o Controlo Web é automaticamente activado e configurado para bloquear o acesso aos sítios de Internet considerados inadequados para a idade do seu filho.

Para configurar o Controlo Web para uma determinada conta de utilizador:

1. Aceda à janela de definições do Controlo Parental BitDefender para a conta desse utilizador.
2. Clique no separador **Web**.
3. Utilize o botão para activar o Controlo Web.
4. Pode verifi9car que categorias web foram automaticamente bloqueadas/restringidas para a classe etária actualmente seleccionada.Se não está satisfeito com as predefinições, pode configurar manualmente.

   Para alterar a acção configurada para uma determinada categoria de conteúdo web, clique no estado actual e seleccione a acção pretendida no menu.
5. Se desejar, crie as suas próprias regras para permitir ou bloquear o acesso a determinados sítios de Internet.Se o Controlo Parental bloquear automaticamente

o acesso a um sítio de Internet, pode criar uma regra para explicitamente permitir o acesso a esse sítio.

6. Pode definir os limites do tempo que os seus filhos passam na Internet.Para mais informação, por favor consulte o "Restringir o Acesso à Internet por Tempo" (p. 110).

Criar Regras de Controlo Web

Para permitir ou bloquear acesso a um website, siga estes passos:

1. Clique em **Permitir Sítio** ou **Bloquear Sítio**.
2. Entre no endereço do website no **campo do Website**.
3. Seleccione a acção desejada para esta regra - **Permitir** ou **Bloquear**.
4. Clique em **Terminar** para adicionar a regra.

Gerir Regras de Controlo Web

As regras de Controlo de Sítios de Internet que já foram configuradas estão listadas na tabela que se encontra na parte inferior da janela. O endereço do sítio de Internet e o estado actual estão listados para cada regra de Controlo Web.

Para eliminar uma regra, seleccione-a e clique em **Remover**.

Para editar uma regra, seleccione-a e clique em **Editar** ou faça duplo-clique sobre ela.Faça as alterações necessárias na janela de configuração.

Restringir o Acesso à Internet por Tempo

Na secção Agendar o Acesso à Internet, pode limitar o tempo que os seus filhos passam na Internet.

Para bloquear totalmente o acesso à Internet, seleccione **Bloquear Acesso à Internet**.

Para restringir o acesso à Internet para determinadas horas do dia:

1. Seleccione **Limitar o tempo de acesso à Internet**.
2. Clique em **Mudar Agendamento**.
3. Seleccione na grelha os intervalos de tempo em que o acesso à Internet está bloqueado.Pode clicar em células individuais, ou pode clicar e arrastar o rato para abranger períodos maiores.
4. Clique em **Guardar**.

Nota

O BitDefender vai efectuar actualizações a cada hora independentemente de o acesso à Internet estar bloqueado.

19.1.3. Controlo de Aplicação

O **Controlo de aplicações** ajuda-o a bloquear qualquer programa impedindo-o de se executar. Jogos, software de multimédia e de mensagens, assim como outras categorias de software e malware podem ser bloqueadas desta forma. As aplicações bloqueadas desta forma ficam também protegidas de modificações, e não podem ser copiadas ou movidas.Pode bloquear permanentemente as aplicações ou apenas durante um intervalo de tempo, tais como os que os seus filhos utilizam para fazer os trabalhos de casa.

Para configurar o Controlo de Aplicações para uma determinada conta de utilizador:

1. Aceda à janela de definições do Controlo Parental BitDefender para a conta desse utilizador.
2. Clique no separador **Aplicações**.
3. Utilize o botão para activar o Controlo de Aplicações.
4. Crie regras para as aplicações para as quais que pretende bloquear ou restringir o acesso.

Criar Regras de Controlo de Aplicações

Para bloquear ou restrinjir acesso a uma aplicação, siga estes passos:

1. Clique em **Bloquear Aplicação** ou **Restringir Aplicação**.
2. Clique em **Explorar** para localizar a aplicação a que quer bloquear/restringir o acesso.As aplicações instaladas estão, normalmente, localizadas na pasta `C:\Programas`.
3. Seleccionar a acção da regra:
   - **Bloquear permanentemente** para bloquear completamente o acesso à aplicação.
   - **Bloqueia baseado nesta agenda** para restrinjir o acesso a determinados intervalos de tempo.

   Se optar por restringir o acesso em vez de bloquear completamente a aplicação, deve também escolher a partir de que dia e intervalos de tempo é que o acesso é bloquado.
4. Clique em **Guardar** para adicionar a regra.

Gerir Regras de Controlo de Aplicações

As regras de Controlo de Aplicação que já foram configuradas estão listadas na tabela que se encontra na parte inferior da janela. O nome da aplicação, o caminho e o estado actual estão listados para cada regra de Controlo de Aplicação.

Para eliminar uma regra, seleccione-a e clique em **Remover**.

Para editar uma regra, seleccione-a e clique em **Editar** ou faça duplo-clique sobre ela.Faça as alterações necessárias na janela de configuração.

19.1.4. Controlo de Palavras-Chave

A Filtragem por Palavra-chave ajuda-o a bloquear o acesso dos utilizadores a mensagens de e-mail, páginas web e mensagens instântaneas que contenham determinadas palavras.Ao usar a Filtragem por Palavra-chave, pode evitar que as crianças vejam palavras ou frases inapropriadas quando estão on-line.

Nota
A Filtragem por Palavra-chave das mensagens instântaneas só está disponível para o Yahoo Messenger e o Windows Live (MSN) Messenger.

Para configurar o Controlo de Palavras-Chave para uma determinada conta de utilizador:

1. Aceda à janela de definições do Controlo Parental BitDefender para a conta desse utilizador.
2. Clique no separador **Palavras-Chave**.
3. Utilize o botão para activar o Controlo de Palavras-Chave.
4. Crie regras de Controlo de Palavras-Chave para bloquear palavras inadequadas.
5. Para impedir que os seus filhos forneçam informações pessoais (como a morada ou o número de telefone) a pessoas que conheceram na Internet, tem de criar regras de Controlo de Identidade.Para mais informação, por favor consulte o "Criar Regras de Controlo de Identidade" (p. 113).

Criar Regras de Controlo de Palavras-chave

Para bloquear uma palavra ou frase, siga estes passos:

1. Clique em **Bloquear Palavra-Chave**.
2. Escreva a palavra ou frase que deseja bloquear no campo editar. Se somente quiser que sejam detectadas palavras inteiras, selecione o **Igualar Todas as Palavras** check box.
3. Seleccione o tipo de tráfego que o BitDefender deverá analisar para essa palavra específica.

Opção	Descrição
HTTP	As páginas web que contenham a palavra-chave são bloqueadas.
POP3	As mensagens de e-mail que contenham a palavra-chave são bloqueadas.

Opção	Descrição
Mensagens Instântaneas	As mensagens instântaneas que contenham a palavra-chave são bloqueadas.

4. Clique em **Terminar** para adicionar a regra.

Gerir Regras de Controlo de Palavras-Chave

As regras de Controlo de Palavras-Chave que foram configuradas estão enumeradas na tabela. É apresentada informação detalhada para cada regra.

Para eliminar uma regra, seleccione-a e clique em **Remover**.

Para editar uma regra, seleccione-a e clique em **Editar** ou faça duplo-clique sobre ela.Faça as alterações necessárias na janela de configuração.

Criar Regras de Controlo de Identidade

Para criar uma regra de Controlo de Identidade, clique no respectivo botão **Bloquear Palavra-Chave** e siga as instruções do assistente de configuração.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Janela de boas-vindas**
2. **Definir Tipo de Regra e Dados**

   Deve definir os seguintes parâmetros:

   - **Nome Regra** - insira o nome da regra no campo editável.
   - **Tipo de Regra** - escolha o tipo de regra (morada, nome, cartão de crédito, PIN, NSS, etc.
   - **Dados Regra** - insira os dados que quer proteger com a regra no campo editável.Por exemplo, se deseja proteger o seu número de cartão de crédito, insira o mesmo ou parte dele aqui.

   Importante

   Se inserir menos do que três caracteres, será notificado a validar os dados. Recomendamos que insira pelo menos três caracteres de forma a evitar o bloqueio por engano de mensagens e páginas web.

   Todos os dados que inserir são encriptados. Para uma segurança adicional, não insira a totalidade dos dados que deseja proteger.

3. **Seleccione Opções de Análise**

   Seleccione o tráfego que quer que o BitDefender analise.

- **Analisar Web (tráfego HTTP)** - analisa o tráfego HTTP (web) e bloqueia os dados de saída que correspondem aos dados da regra.
- **Analisar e-mail (tráfego SMTP)** - analisa todo o tráfego SMTP (mail) e bloqueia as mensagens de e-mail de saída que contém os dados da regra.
- **Analisar Mensagens Instantâneas** - analisa todo o tráfego Mensagens Instantâneas e bloqueia as mensagens de chat de saída que contenham os dados da regra.

Pode escolher aplicar a regra apenas se a mesma corresponder em todas as palavras ou se os dados da regra e os caracteres detectados correspondem em termos de letra (Maiúsculas, minúsculas).

4. **Descrever Regra**

   Insira uma breve descrição da regra no campo de edição.Um vez que os dados bloqueados (string de caracteres) não são mostrados em pleno texto quando se acede à regra, a descripção deverá ajudá-lo a identificá-la facilmente.

   Clique em **Terminar**.A regra aparecerá na tabela.

A partir se agora, qualquer tentativa para enviar os dados especificados (por correio electrónico, mensagens electrónicas ou páginas da Internet) irá falhar. Será apresentada uma mensagem de alerta indicando que o BitDefender impediu o envio de elementos de identificação.

19.1.5. Controlo de Mensagens Instântaneas (IM)

O Controlo de Mensagens Instântaneas (IM) permite-lhe especificar os contactos IM com os quais a sua criança pode fazer chat.

Nota

O Controlo de Mensagens Instântaneas (IM) só está disponível para o Yahoo Messenger e o Windows Live (MSN) Messenger.

Para configurar o Controlo de MI para uma determinada conta de utilizador:

1. Aceda à janela de definições do Controlo Parental BitDefender para a conta desse utilizador.
2. Clique no separador **Mensagens Instantâneas**.
3. Utilize o botão para activar o Controlo de Mensagens Instantâneas.
4. Seleccione o método de filtro preferido e, consoante a sua escolha, crie as regras apropriadas.
   - **Permitir MI com todos os contactos, excepto aqueles na lista**

     Neste caso, tem de especificar os IDs de MI a bloquear (pessoas com que os seus filhos não devem falar).

- **Bloquear MI com todos os contactos, excepto aqueles na lista**

  Neste caso, tem de especificar os IDs de MI com quem os seus filhos estão autorizados a trocar mensagens instantâneas.Por exemplo, pode permitir a troca de mensagens instantâneas com membros de família, amigos da escola ou vizinhos.

  Esta segunda opção é recomendada se o seu filho tiver menos de 14 anos.

Criando Regras de Controlo de Mensagens Instantâneas (MI)

Para permitir ou bloquear as mensagens instantâneas com um contacto, siga estes passos:

1. Clique em **Bloquear ID de MI** ou **Permitir ID de MI**.
2. Digite o endereço de e-mail ou o nome de utilizador usado pelo contacto do IM no campo **E-mail ou ID IM** .
3. Escolher o program de IM com o qual o contacto se associa.
4. Seleccione a acção desejada para esta regra - **Permitir** ou **Bloquear**.
5. Clique em **Terminar** para adicionar a regra.

Gerindo Regras de Controlo de Mensagens Instantâneas (MI)

As regras do Controlo de MI que foram configuradas estão listadas na tabela ao fundo da janela.

Para eliminar uma regra, seleccione-a e clique em **Remover**.

Para editar uma regra, seleccione-a e clique em **Editar** ou faça duplo-clique sobre ela.Faça as alterações necessárias na janela de configuração.

19.2. Monotorizar Actividade das Crianças

BitDefender ajuda-o a acompanhar o que seus filhos estão a fazer no computador, mesmo quando está ausente.

Por defeito, quando o Controlo Parental está activado, as actividades dos seus filhos são registadas. Desta forma, consegue sempre ver os sítios de Internet que visitaram, as aplicações que utilizaram, as actividades bloqueadas pelo Controlo Parental, etc.

Também pode configurar o BitDefender para enviar notificações por correio electrónico quando o Controlo Parental bloqueia uma actividade.

19.2.1. Consultar os Relatórios do Controlo Parental

Para ver o que os seus filhos fizeram recentemente no computador, consulte os relatórios do Controlo Parental.Siga estes passos:

1. Abrir o BitDefender.

2. Clique na hiperligação **Ver Relatórios** que se encontra no canto inferior direito da janela.
3. Clique em **Controlo Parental** no menu do lado esquerdo.

Nota

Também pode abrir esses relatórios na janela do Controlo Parental clicando em **Ver Relatórios**.

Se não quiser utilizar o computador com os seus filhos, pode configurar a rede doméstica BitDefender para que possa aceder aos relatórios do Controlo Parental à distância (a partir do seu computador).Para mais informação, por favor consulte o “*A Sua Rede*” (p. 199).

Os relatórios do Controlo Parental fornecem informações pormenorizadas sobre as actividades dos seus filhos no computador e na Internet.A informação é organizada em vários separadores:

Geral

Providencia informações gerais sobre as actividades recentes dos seus filhos, como os sítios de Internet mais visitados e as aplicações mais utilizadas.

Pode filtrar automaticamente por utilizador e período de tempo.

Registo de Aplicações

Ajuda-o a descobrir que aplicações os seus filhos utilizaram recentemente.

Faça duplo clique nos eventos da lista para ver mais detalhes.Para eliminar uma entrada de registo, clique nela com o botão direito e seleccione **Eliminar**.

Registo de Internet

Ajuda-o a descobrir que sítios de Internet os seus filhos visitaram recentemente.

Pode filtrar automaticamente por utilizador e período de tempo.

Outros Eventos

Ajuda a encontrar informações detalhadas sobre a actividade do Controlo Parental (por exemplo, quando o Controlo Parental esteve activado/desactivado, que eventos foram bloqueados).

Faça duplo clique nos eventos da lista para ver mais detalhes.Para eliminar uma entrada de registo, clique nela com o botão direito e seleccione **Eliminar**.

19.2.2. A Configurar Notificações de E-mail

Para receber notificações por correio electrónico quando o Controlo Parental bloqueia uma actividade:

1. Abrir o BitDefender.
2. Consoante o modo do interface de utilizador, aceda ao Controlo Parental da seguinte forma:

Modo Intermédio

Abra o separador **Segurança** e clique em **Controlo Parental**, nas Tarefas Rápidas, no lado esquerdo da janela.

Modo Avançado

Clique em **Controlo Parental** no menu do lado esquerdo.

Nota

No Modo Básico e no Modo Intermédio, pode configurar um atalho para poder aceder a estas definições a partir do painel de instrumentos.Para mais informação, por favor consulte o "*Ferramentas*" (p. 36).

3. NA secção Definições, seleccione **Envie-me um relatório de actividade para o e-mail**.
4. Será solicitado a configurar as definições da sua conta de e-mail. Clique em **Sim** para abrir a janela de configuração.

Nota

Pode abrir a janela de configuração mais tarde ao clicar **Definições de Notificação**.

5. Introduza o endereço electrónico para onde serão enviadas das notificações por correio electrónico.
6. Configure as definições de correio electrónico do servidor utilizado para enviar as notificações electrónicas.

Há três opções para configurar as definições de correio electrónico:

Utilizar as definições do cliente de correio electrónico actual

Esta opção está seleccionada por defeito quando o BitDefender importa as definições do servidor de correio electrónico para o seu cliente de correio.

Clique em **Definições Teste** para validar as definições. Se ocorrer algum problema durante a validação, será informado que tem de as corrigir.

Seleccione um dos servidores conhecidos

Seleccione esta opção se possuir um conta de correio electrónico num dos serviços de correio electrónico baseados na Internet indicados na lista.

Clique em **Definições Teste** para validar as definições. Se ocorrer algum problema durante a validação, será informado que tem de as corrigir.

Quero configurar as definições do servidor

Se souber as definições do servidor de correio electrónico, seleccione esta opção para configurar as definições da seguinte forma:

- **Servidor SMTP de Envio** - digite o endereço do servidor de e-mail utilizado para enviar mensagens e-mail.

- Se o servidor usa uma porta diferente do que o padrão porta 25, digite-o no campo correspondente.
- Se o servidor requer autentificação, seleccione a caixa de selecção **O meu servidor SMTP requer autentificação** e digite o nome de utilizador e palavra-passe nos respectivos campos.

Clique em **Definições Teste** para validar as definições. Se ocorrer algum problema durante a validação, será informado que tem de as corrigir.

Clique em **OK** para guardar as alterações e fechar a janela.

19.3. Controlo Parental Remoto

O Controlo Parental Remoto permite-lhe monitorizar as actividades dos seus filhos e alterar as definições do Controlo Parental, mesmo quando não está em casa.Tudo o que precisa é um computador com acesso à Internet e um navegador de Internet.

O Controlo Parental Remoto providencia uma forma discreta para saber o que os seus filhos fazem na Internet, sem invadir a privacidade.

19.3.1. Pré-Requisitos para Utilizar o Controlo Parental Remoto

Para utilizar o Controlo Parental Remoto, devem ser cumpridos os seguintes pré-requisitos:

1. Instale o BitDefender Internet Security 2011 ou o BitDefender Total Security 2011 no computador dos seus filhos.
2. Active o produto com uma conta BitDefender.
3. Activar o Controlo Parental Remoto.
4. O computador a partir do qual pretende aceder ao Controlo Parental Remoto tem de estar ligado à Internet.

19.3.2. Activar o Controlo Parental Remoto

Para activar o Controlo Parental Remoto:

1. Inicie sessão no computador onde o BitDefender está instalado com uma conta de administrador.Pode utilizar a mesma conta que utilizou para instalar o programa.
2. Abrir o BitDefender.
3. Consoante o modo do interface de utilizador, aceda ao Controlo Parental da seguinte forma:

   Modo Intermédio

   Abra o separador **Segurança** e clique em **Controlo Parental**, nas Tarefas Rápidas, no lado esquerdo da janela.

Modo Avançado
  Clique em **Controlo Parental** no menu do lado esquerdo.

Nota

No Modo Básico e no Modo Intermédio, pode configurar um atalho para poder aceder a estas definições a partir do painel de instrumentos.Para mais informação, por favor consulte o "*Ferramentas*" (p. 36).

4. Utilize o botão para activar o Controlo Parental Remoto.O Controlo Parental Remoto será activado para todas as contas no sistema.

19.3.3. Aceder ao Controlo Parental Remoto

Pode aceder ao Controlo Parental Remoto a partir da sua Conta BitDefender.

1. Num computador com acesso à Internet, abra o navegador da Internet e vá a:

   http://myaccount.bitdefender.com

2. Inicie sessão na sua conta BitDefender com o seu nome de utilizador e palavra-passe.
3. Clique no separador **Controlo Parental** para aceder ao painel de instrumentos do Controlo Parental Remoto.
4. Pode visualizar todas as contas de utilizador para as quais está activado o Controlo Parental Remoto.

   Para verificar as actividades que foram bloqueadas numa determinada conta de utilizador desde o seu último início de sessão, clique na hiperligação que indica a existência de alertas.

   Para ver as actividades recentes dos seus filhos, clique na hiperligação **Actividade Recente** que corresponde à conta deles.

   Para alterar as definições do Controlo Parental de uma determinada conta de utilizador, clique na respectiva hiperligação **Definições**.

19.3.4. Monitorizar as Actividades dos Seus Filhos à Distância

Antes de monitorizar à distância o computador e a actividade na Internet dos seus filhos, tem de activar o Controlo Parental Remoto no computador deles.Para mais informação, por favor consulte o "*Activar o Controlo Parental Remoto*" (p. 118).

Para verificar à distância o que os seus filhos estão a fazer no computador:

1. Num computador com acesso à Internet, abra o navegador da Internet e vá a:

   http://myaccount.bitdefender.com

2. Inicie sessão na sua conta BitDefender com o seu nome de utilizador e palavra-passe.

3. Clique no separador **Controlo Parental** para aceder ao painel de instrumentos do Controlo Parental Remoto.
4. Para verificar as actividades que foram bloqueadas numa determinada conta de utilizador desde o seu último início de sessão, clique na hiperligação que indica a existência de alertas.Para ver as actividades recentes dos seus filhos, clique na hiperligação **Actividade Recente** que corresponde à conta deles.

Na página de Alertas, pode ver que sítios de Internet, aplicações ou contactos de conversação foram bloqueados desde o último início de sessão.

Na página Actividade recente, pode encontrar informações úteis sobre as actividades mais recentes dos seus filhos:

- quais são os sítios de Internet mais acedidos e mais bloqueados.
- quais são as aplicações mais acedidas e mais bloqueadas.
- que são os IDs de conversação mais contactados e mais bloqueados.

Pode bloquear directamente um sítio de Internet, uma aplicação ou um ID de conversação clicando na respectiva hiperligação **Bloquear**.

Para remover uma restrição, clique na respectiva hiperligação **Permitir**.

19.3.5. Alterar as Definições do Controlo Parental à Distância

Antes de alterar à distância as definições do Controlo Parental configuradas para os seus filhos, tem de activar o Controlo Parental Remoto no computador deles.Para mais informação, por favor consulte o “*Activar o Controlo Parental Remoto*” (p. 118).

Para alterar as definições do Controlo Parental à distância:

1. Num computador com acesso à Internet, abra o navegador da Internet e vá a:

   http://myaccount.bitdefender.com
2. Inicie sessão na sua conta BitDefender com o seu nome de utilizador e palavra-passe.
3. Clique no separador **Controlo Parental** para aceder ao painel de instrumentos do Controlo Parental Remoto.
4. Pode visualizar todas as contas de utilizador para as quais está activado o Controlo Parental Remoto.Para alterar as definições do Controlo Parental de uma determinada conta de utilizador, clique na respectiva hiperligação **Definições**.

A página de Definições apresenta os sítios de Internet, as aplicações e os IDs das mensagens instantâneas que são explicitamente bloqueados pelo Controlo Parental.Para remover uma restrição, clique na respectiva hiperligação **Permitir**.

Para saber como definir restrições, por favor consulte os seguintes tópicos:

“Restringir o Acesso à Internet por Tempo” (p. 121)

"Bloquear Sítios de Internet" (p. 121)
"Bloquear Aplicações" (p. 121)
"Bloquear Contactos MI" (p. 122)

Restringir o Acesso à Internet por Tempo

Escolha uma opção no menu para especificar quando o seu filho está autorizado a aceder à Internet.Para restringir o acesso à Internet para determinadas horas do dia:

1. Seleccione **Agendar Aceso à Internet**.
2. Seleccione na grelha os intervalos de tempo em que o acesso à Internet está bloqueado.Pode clicar em células individuais, ou pode clicar e arrastar o rato para abranger períodos maiores.Para iniciar uma nova selecção, clique em **Bloquear Todos** ou **Permitir Todos**.
3. Clique em **Submeter Alterações**.As alterações serão configuradas e aplicadas no computador do seu filho após a próxima sincronização com o sítio de Internet do Controlo Parental Remoto (intervalo máximo de 10 minutos).

Bloquear Sítios de Internet

Para bloquear um sítio de Internet:

1. Clique em **Bloquear outro sítio de Internet**.
2. Introduza o sítio de Internet no respectivo campo. Em alternativa, se quiser bloquear um dos sítios de Internet mais visitados, seleccione-o no menu.
3. Clique em **Bloquear**.O sítio de Internet será adicionado à lista de sítios bloqueados.A regra será configurada e aplicada no computador do seu filho após a próxima sincronização com o sítio de Internet do Controlo Parental Remoto (intervalo máximo de 10 minutos).

Se mudar de ideias, clique na respectiva hiperligação **Permitir**.

Bloquear Aplicações

Para bloquear uma aplicação:

1. Clique em **Bloquear outra aplicação**.
2. Seleccione a aplicação a bloquear na lista das aplicações mais utilizadas.
3. Clique em **Bloquear**.A aplicação será adicionada à lista de aplicações bloqueadas.A regra será configurada e aplicada no computador do seu filho após a próxima sincronização com o sítio de Internet do Controlo Parental Remoto (intervalo máximo de 10 minutos).

Se mudar de ideias, clique na respectiva hiperligação **Permitir**.

Bloquear Contactos MI

Para bloquear mensagens instantâneas de um contacto específico:

1. Clique em **Bloquear outro contacto**.
2. Introduza o ID de mensagens instantâneas no campo correspondente. Em alternativa, se quiser bloquear um dos IDs mais frequentemente contactados, seleccione-o no menu.
3. Clique em **Bloquear**.O ID de conversação será adicionado à lista de IDs bloqueados.A regra será configurada e aplicada no computador do seu filho após a próxima sincronização com o sítio de Internet do Controlo Parental Remoto (intervalo máximo de 10 minutos).

Se mudar de ideias, clique na respectiva hiperligação **Permitir**.

20. Controlo de Privacidade

BitDefender monitoriza dezenas de potenciais “hotspots” no seu sistema onde o spyware poderá actuar, e também verifica quaisquer mudanças feitas ao seu sistema e ao seu software. É bastante eficaz no bloqueio de cavalos de Tróia e outras ferramentas instaladas por hackers, que tentam comprometer a sua privacidade e enviar a sua informação pessoal, tal como números de cartão de crédito, do seu computador para o do hacker.

O Controlo de Privacidade inclui os seguintes componentes:

- Controlo de Identidade - ajuda a garantir que os seus dados pessoais não são enviados a partir do computador sem o seu consentimento. Analisa as mensagens electrónicas e instantâneas enviadas do computador, assim como todos os dados enviados através de páginas da Internet, e bloqueia toda a informação protegida pelas regras de Controlo de Identidade que criou.
- O Controlo do Registo - irá pedir a sua permissão sempre que um programa tentar modificar uma entrada de registo de forma a poder ser executado durante o arranque do Windows.
- O Controlo de Cookies - irá pedir a sua permissão sempre que um novo site web tentar definir uma cookie.
- O Controlo de script - irá pedir a sua permissão sempre que um site web tente activar um script ou outro conteúdo activo.

Por defeito, apenas o Controlo de Identidade está activado.Tem de configurar correctamente as regras do Controlo de Identidade para impedir o envio não autorizado de informações confidenciais.Para mais informação, por favor consulte o “*Configurar o Controlo de Identidade*” (p. 125).

Os outros componentes do Controlo de Privacidade são interactivos. Se os activar, ser-lhe-á pedido, em janelas de alerta, que autorize ou bloqueie certas acções quando estiver a navegar na Internet ou a instalar novo software. É por isso que é, normalmente, utilizado por utilizadores mais experientes.

20.1. Configurar Nível de Protecção

O nível de protecção ajuda-o a activar ou desactivar facilmente os componentes do Controlo de Privacidade.

Para configurar o nível de protecção:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Controlo de Privacidade > Estado**.
3. Certifique-se que o Controlo de Privacidade está activado.

4. Há duas opções:
   - Arraste o cursor pela escala para definir o nível de protecção apropriada.Clique em **Nível por Defeito** para colocar o mostrador no nível por defeito.

     Utilize a descrição do lado direito da escala para escolher o nível de protecção que melhor se adequa às suas necessidades de segurança.
   - Pode personalizar o nível de protecção clicando em **Nível Pessoal**.Na janela que lhe irá aparecer, escolha o controlos de protecção que deseja activar e clique em **OK**.

20.2. Controlo de identidade

O Controlo de Identidade protege-o contra o roubo de informação sensível quando se encontra on-line.

Imagine a seguinte situação: criou uma regra de Controlo de Identidade para proteger o número do seu cartão de crédito.Se, de alguma forma, um software espião conseguir instalar-se no seu computador, não conseguirá enviar o número do seu cartão de crédito em mensagens de correio electrónico, mensagens instantâneas ou páginas de Internet. Além disso, os seus filhos não poderão utilizá-lo para fazer compras em linha ou revelá-lo a pessoas que conheceram na Internet.

Para saber mais, consulte os seguintes tópicos:

- "*Sobre o Controlo de Identidade*" (p. 124).
- "*Configurar o Controlo de Identidade*" (p. 125).
- "*Gerir Regras*" (p. 128).

20.2.1. Sobre o Controlo de Identidade

Manter informação confidencial segura é um assunto importante que nos preocupa a todos. O roubo de dados tem crescido com o desenvolvimento das comunicações Internet e actualmente fazem-se uso de novos métodos para enganar as pessoas e retirar-lhes informação privada.

Quer seja o seu e-mail o seu número de cartão de crédito, quandos eles caem em mãos erradas essa informação poderá causar-lhe danos: poderá encontrar-se afogado em mensagens spam ou poderá ser surpreendido ao aceder à sua conta e verificar que está vazia.

O Controlo de Identidade protege-o contra o roubo de informação sensível quando se encontra on-line.Baseado nas regras que criar, o Controlo de Identidade analisa o tráfego web, de e-mail e de mensagens instantâneas que sai do seu computador em busca de chaves de caracteres específicos (por exemplo, o seu número de cartão de crédito). Se houver uma correspondência, a respectiva página web, e-mail ou mensagem instantânea é bloqueada.

Pode criar regras para proteger cada peça de informação que possa considerar pessoal ou confidencial, desde o seu número de telefone ou endereço de e-mail até à sua informação bancária.Suporte multi-utilizador é fornecido de forma a que os utilizadores de diferentes contas do Windows possam configurar e usar as suas próprias regras de identidade.Se a sua conta de Windows é uma conta de administrador, as regras que cria podem ser configuradas para também se aplicarem a utilizadores de outras contas do computador.

Porquê usar o Controlo de Identidade?

- O Controlo de Identidade é bastante eficaz a bloquear spyware keylogger.Este tipo de aplicações maliciosas grava as teclas que pressionou no teclado e envia-as para a Internet para uma pessoa maliciosa (hacker).O hacker pode descobrir informação sensível a partir de dados roubados, tais como números de contas bancárias e palavras-passe, e usá-las em benefício pessoal.

  Supondo que tal aplicação funciona de forma a evitar a detecção antivírus, a mesma não pode enviar os dados roubados por e-mail, web ou mensagens instântaneas se tiver criado as regras de protecção de identidade adequadas.

- O Controlo de Identidade protege-o contra as tentativas de phishing (tentativas de roubar informação pessoal).As tentativas de phishing mais comuns fazem uso de um e-mail enganador para o levar a inserir informação pessoal numa página web falsa.

  Por exemplo, poderá receber um e-mail a fingir que é do seu banco a pedir-lhe que actualize os dados da sua conta bancária com urgência.O e-mail traz um link para uma página web onde deve de inserir a sua informação pessoal.Apesar de parecerem legítimos, o e-mail e o link para a página web são falsos.Se clicar no link do e-mail e inserir a sua informação pessoal na página web falsa, estará a revelar esta informação às pessoas maliciosas que organizaram a tentativa de phishing.

  Se as regras de protecção de identidade estiverem feitas, não poderá enviar informação pessoal (tal como o número do seu cartão de crédito) para uma página web a não ser que tenha definido essa página web como uma excepção.

- Com as regras do Controlo de Identidade, pode evitar que os seus filhos forneçam informações pessoais (por exemplo, a morada ou o número de telefone) a pessoas que conheceram na Internet. Além disso, se criar regras para proteger o seu cartão de crédito, eles não poderão fazer compras sem o seu consentimento.

20.2.2. Configurar o Controlo de Identidade

Se deseja usar p Controlo de Identidade, siga estes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Controlo de Privacidade > Identidade**.

3. Certifique-se que o Controlo de Identidade está activado.

Nota
Se não for possível configurar a opção, vá ao separador **Estado** e active o Controlo de Privacidade.

4. Criar regras para proteger a sua informação sensível.Para mais informação, por favor consulte o “*Criar Regras de Controlo de Identidade*” (p. 126).
5. Se necessário, defina excepções específicas para as regras que criou.Por exemplo, se criou uma regra para proteger o número do seu cartão de crédito, adicione os sítios de Internet onde normalmente utiliza o cartão de crédito à lista de exclusões.Para mais informação, por favor consulte o “*Definir Excepções*” (p. 127).

Criar Regras de Controlo de Identidade

Para criar uma regra de protecção de identidade clique no botão **Adicionar** e siga o assistente de configuração.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Janela de boas-vindas**
2. **Definir Tipo de Regra e Dados**

   Deve definir os seguintes parâmetros:

   - **Nome Regra** - insira o nome da regra no campo editável.
   - **Tipo de Regra** - escolha o tipo de regra (morada, nome, cartão de crédito, PIN, NSS, etc.
   - **Dados Regra** - insira os dados que quer proteger com a regra no campo editável.Por exemplo, se deseja proteger o seu número de cartão de crédito, insira o mesmo ou parte dele aqui.

   Importante
   Se inserir menos do que três caracteres, será notificado a validar os dados. Recomendamos que insira pelo menos três caracteres de forma a evitar o bloqueio por engano de mensagens e páginas web.

   Todos os dados que inserir são encriptados. Para uma segurança adicional, não insira a totalidade dos dados que deseja proteger.

3. **Seleccione Utilizadores e Tipo de Trafego.**

   a. Seleccione o tráfego que quer que o BitDefender analise.

   - **Analisar Web (tráfego HTTP)** - analisa o tráfego HTTP (web) e bloqueia os dados de saída que correspondem aos dados da regra.

- **Analisar e-mail (tráfego SMTP)** - analisa todo o tráfego SMTP (mail) e bloqueia as mensagens de e-mail de saída que contém os dados da regra.
- **Analisar Mensagens Instantâneas** - analisa todo o tráfego Mensagens Instantâneas e bloqueia as mensagens de chat de saída que contenham os dados da regra.

Pode escolher aplicar a regra apenas se a mesma corresponder em todas as palavras ou se os dados da regra e os caracteres detectados correspondem em termos de letra (Maiúsculas, minúsculas).

b. Específique para que utilizadores se aplicam as regras.

- **Apenas para mim (utilizador actual)** - a regra será aplicada à sua conta de utilizador.
- **Utilizadores limitados** - a regra será aplicada a si e a todas as contas de Windows limitadas.
- **Todos os utilizadores** - a regra será aplicada a todas contas do Windows.

4. **Descrever Regra**

   Insira uma breve descrição da regra no campo de edição.Um vez que os dados bloqueados (string de caracteres) não são mostrados em pleno texto quando se acede à regra, a descripção deverá ajudá-lo a identificá-la facilmente.

   Clique em **Terminar**.A regra aparecerá na tabela.

A partir se agora, qualquer tentativa para enviar os dados especificados (por correio electrónico, mensagens electrónicas ou páginas da Internet) irá falhar. Será apresentada uma mensagem de alerta indicando que o BitDefender impediu o envio de elementos de identificação.

Definir Excepções

Há casos em que necessita de definir excepções para especificar as regras de identidade.Consideremos o caso em que criou uma regra que evita que o número do seu cartão de crédito seja enviado por HTTP (web). Sempre que o seu cartão de crédito seja submetido num site web a partir da sua conta de utilizador, a respectiva página web é bloqueada. Se deseja por exemplo, pagar uma compra online numa loja virtual (que você sabe ser segura), terá de especificar uma excepção para a respectiva regra.

Para abrir a janela onde pode gerir as excepções, clique em **Excepções**.

Para adicionar uma excepção, siga os seguintes passos:

1. Clique no botão **Adicionar** para adicionar a nova entrada à tabela.
2. Duplo-clique em **Especificar item excluído** e inserir o endereço web, endereço de e-mail ou o contacto IM que deseja adicionar como excepção.

3. Duplo-clique em**Tipo de Tráfego** e escolha do menu a opção correspondente ao tipo de endereço que inseriu anteriormente.
   - Se especificou um endereço web, seleccione **HTTP**.
   - Se especificou um endereço de e-mail, seleccione **Email (SMTP)**.
   - Se especificou um contacto IM, seleccione**IM**.

Para remover uma excepção da lista, seleccione-a e clique em **Remover**.

Clique em **Aplicar** para guardar as alterações.

20.2.3. Gerir Regras

Para gerir as regras do Controlo de Identidade:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Controlo de Privacidade > Identidade**.

Pode ver as regras criadas até agora listadas na tabela.

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.

Para editar uma regra, seleccione-a e clique no botão **Editar** ou faça duplo-clique sobre ela. Uma nova janela irá aparecer.Aqui pode mudar o nome, descripção e parâmetros da regra (tipo, dados e tráfego). Clique em **OK** para guardar as alterações.

20.3. Controlo de registo

Uma parte muito importante do sistema operativo do Windows é chamada de **Registo**. Aqui é o local onde o guarda as suas definições, programas instalados, informação acerca do utilizador e por aí a diante.

O **Registo** também é utilizado para definir quais os programas que deverão ser lançados automaticamente ao iniciar o Windows. Frequentemente, os vírus usam isto para se lançarem automaticamente quando o utilizador reiniciar o seu computador.

O **Controlo de registo** vigia o Registo do Windows – mais uma vez, isto é útil para detectar Cavalos de Tróia. Irá alertá-lo sempre que um programa tente modificar uma entrada de registo para poder ser executado ao iniciar o Windows.Para mais informação, por favor consulte o “*Alertas de Registo*” (p. 43).

Para configurar o Controlo de Registo:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Controlo de Privacidade > Registo**.
3. Seleccione a caixa respectiva para activar o Controlo de Registo.

Nota
Se não for possível configurar a opção, vá ao separador **Estado** e active o Controlo de Privacidade.

Gerir Regras

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.

20.4. Controlo de cookies

As Cookies são uma ocurrência muito comum na Internet. Elas são ficheiros peqenos armazenados no seu computador. Os sites da Web criam estas cookies para manter o rasto da informação específica acerca de si.

As Cookies são geralmente criadas para facilitar a sua vida. Por exemplo, elas podem ajudar o site da Web a lembrar-se do seu nome e preferências, para que não tenha de as voltar a introduzir sempre que os visitar.

Mas as cookies também podem ser usadas para comprometer a sua privacidade, ao seguir o rasto das patentes da sua navegação.

É aqui que o Controlo de Cookies ajuda.Quando activado, o Controlo de Cookies vai pedir-lhe autorização sempre que um novo sítio de Internet tenta definir ou pedir um cookie.Para mais informação, por favor consulte o “*Alertas de Cookie*” (p. 44).

Para configurar o Controlo de Cookies:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Controlo de Privacidade > Cookie**.
3. Seleccione a caixa respectiva para activar o Controlo de Cookies.

Nota
Se não for possível configurar a opção, vá ao separador **Estado** e active o Controlo de Privacidade.

4. Pode configurar as regras para os sítios de Internet que visita regularmente, mas isto não é obrigatório.As regras são automaticamente criadas na janela de alertas, com base na sua resposta.

Nota
Devido ao grande número de cookies usadas hoje na Internet, o **Controlo de Cookie** pode ser um pouco aborrecido ao começo. Inicialmente, irá perguntar uma série de questões acerca de sites que tentam colocar cookies no seu computador. Logo que adicione os seus sites habituais à lista-regra, a navegação tornar-se-á tanto facilitada como anteriormente.

Criar Regras Manualmente

Para adicionar manualmente uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.Pode definir os parâmetros:

- **Endereço de domínio** - introduza o domínio, no qual a regra deve aplicar-se.
- **Acção** - selecciona a acção da regra.

Acção	Descrição
Permitir	Os cookies desse domínio serão executados.
Bloquear	Os cookies desse domínio não serão executados.

- **Sentido** - selecciona o sentido do tráfego.

Tipo	Descrição
Saída	A regra será aplicada apenas às cookies que são enviadas para fora do site conectado.
Entrada	A regra será aplicada apenas às cookies que são recebidas do site conectado.
Ambos	A regra aplica-se em ambos os sentidos.

Nota
Pode aceitar cookies mas nunca as poderá devolver, ao estabelecer a acção para **Negar** e a direcção para **Saída**.

Clique em **Terminar**.

Gerir Regras

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.Para alterar os parametros de uma regra, seleccione a regra no botão **Editar** ou faça duplo clique. Faça as alterações desejadas na janela de configuração.

20.5. Controlo de script

Escritas e outros códigos tais como Controlos de ActiveX e Java applets, os quais são usados para criar páginas da web interactivas, podem ser programados para ter efeitos inofensivos. Os elementos do ActiveX, por exemplo, podem ganhar total acesso aos seus dados e podem ler dados do seu computador, informação eliminada, capturar palavras-passe e interceptar mensagens enquanto você está em linha. Apenas deverá aceitar conteúdo activo de sites que conhece e confia totalmente.

Se activar o Controlo de Scripts, ser-lhe-á pedida autorização sempre que um novo sítio de Internet tentar executar um script ou outro conteúdo activo.Para mais informação, por favor consulte o *"Alertas de Script"* (p. 44).

Para configurar o Controlo de Script:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Controlo de Privacidade > Script**.
3. Seleccione a caixa respectiva para activar o Controlo de Script.

Nota
Se não for possível configurar a opção, vá ao separador **Estado** e active o Controlo de Privacidade.

4. Pode configurar as regras para os sítios de Internet que visita regularmente, mas isto não é obrigatório.As regras são automaticamente criadas na janela de alertas, com base na sua resposta.

Criar Regras Manualmente

Para adicionar manualmente uma regra, clique no botão **Adicionar** e configure os parâmetros da regra na janela de configuração.Pode definir os parâmetros:

- **Endereço de domínio** - introduza o domínio, no qual a regra deve aplicar-se.
- **Acção** - selecciona a acção da regra.

Acção	Descrição
Permitir	Os scripts desse domínio serão executados.
Bloquear	Os scripts desse domínio não serão executados.

Clique em **Terminar**.

Gerir Regras

Para apagar uma regra, apenas seleccione-a e clique no botão **Apagar**.Para alterar os parametros de uma regra, seleccione a regra no botão **Editar** ou faça duplo clique. Faça as alterações desejadas na janela de configuração.

21. Firewall

A Firewall protege o seu computador de tentativas de ligações internas e externas não-autorizadas. É bastante semelhante a um guarda que está à sua porta – irá manter um olhar atento na sua ligação à Internet e rastrear a quem permitir e a quem bloquear o acesso à mesma.

Nota
A firewall é essencial se tiver uma ligação de banda larga ou ADSL.

Em Modo Stealth o seu computador fica “escondido” do software maligno e dos hackers. O módulo da firewall é capaz de detectar e proteger automaticamente o seu computador contra os scans de portas (conjunto de pacotes enviados para uma máquina de forma a encontrar "pontos de acesso", frequentemente como modo de preparação para um ataque).

21.1. Definições da Protecção

Para activar/desactivar e configurar a protecção da firewall, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Segurança** e clique em **Configurar a Firewall**, nas Tarefas Rápidas, no lado esquerdo da janela.Seleccione o separador **Definições** na nova janela que aparece.

Modo Avançado
: Vá a **Firewall > Definições**.

Importante
Para se manter protegido contra os ataques da Internet, mantenha activa a **Firewall**.

No cimo da secção, poderá ver várias estatísticas relativas à actividade detectada.

No final desta secção pode ver as estatísticas do BitDefender com respeito ao tráfego de entrada e de saída. O gráfico mostra-lhe o volume de tráfego da Internet durante os últimos dois minutos.

Nota
O gráfico só é apresentado no Modo Avançado.

21.1.1. Definir a Acção por Defeito

Por defeito o BitDefender permite automaticamente que todos os programas conhecidos da sua lista branca acedam aos serviços da rede e à Internet.Para todos

os outros programs o BitDefender consulta-o através de uma janela de alerta para que decida a acção a tomar.A acção que determinar será aplicada cada vez que a respectiva aplicação solicite o acesso à rede/internet.

Arraste o marcador ao longo da escala para definir a acção a ser levada a cabo para as aplicações que solicitem acesso à rede/Internet.

- Permitir todos
- Programas Conhecidos
- Relatório
- Bloquear todas

Quando selecciona uma acção, é apresentada uma breve explicação.

21.1.2. Configuração Avançada da Firewall

No Modo Avançado pode configurar as definições avançadas da firewall clicando em **Definições Avançadas**.

Estão disponíveis as seguintes opções:

- **Activar Suporte de Internet Connection Sharing (ICS)** - activa o suporte para Internet Connection Sharing (ICS).

Nota

Esta opção não activa automaticamente o ICS no seu sistema, mas apenas permite este tipo de ligação em caso de a activar no seu sistema operativo.

- **Detectar aplicações que mudaram desde que a regra da firewall foi criada** - verifica cada aplicação que se tenta ligar à Internet para ver se ela mudou desde que a regra que controla o seu acesso foi adicionada. Se a aplicação foi alterada, uma alerta aparecerá para que permita ou bloqueie o acesso dessa aplicação à Internet.

Nota

As aplicações poderão ser alteradas por malware.Recomendamos que mantenha esta opção seleccionada e permita acesso apenas àquelas aplicações que espera que tenham mudado após a regra que controla o seu acesso ter sido criada.

Aplicações assinadas são suposta serem fiáveis e de um alto nível de segurança.Pode escolher **Ignorar mudanças em processos assinados** de forma a permitir que aplicações assinadas que se alteraram se liguem à Internet sem ser alertado acerca deste evento.

- **Activar notificações wireless** - se estiver ligado a uma rede wireless, mostra janelas informativas com respeito aos eventos de rede (por exemplo, quando um novo computador foi ligado à rede).

- **Bloquear scans de portas** - detecta e bloqueia todas as tentativas de descobrir que portas se encontram abertas.

  Os scans de portas são frequentemente usados pelos hackers para descobrir que portas se encontram abertas no seu computador.Então eles poderão entrar no seu computador se descobrirem uma porta menos segura ou vulnerável.
- **Regras automáticas estritas** - cria regras estritas usando a janela de alerta da firewall.Com esta opção seleccionada. o BitDefender consulta-lo-á para tomar uma acção e criar regras para cada diferente processo que abre a aplicação que está a solicitar o acesso à rede ou à Internet.

21.2. Regras de Acesso a Aplicações

Para gerir as regras da firewall que controlam o acesso das aplicações a serviços de rede e à Internet, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Segurança** e clique em **Configurar a Firewall**, nas Tarefas Rápidas, no lado esquerdo da janela.Seleccione o separador **Programas** na nova janela que aparece.

Modo Avançado
: Vá a **Firewall > Programas**.

O Modo Intermédio dá acesso às definições da configuração básica. Para aceder a opções de personalização, utilize o Modo Avançado.

21.2.1. Ver Regras Actuais

Pode ver na tabela os programas (processos) para os quais as regras de firewall foram criadas.

No Modo Avançado, pode ficar a saber informações detalhadas sobre cada regra, como indicado pelas colunas da tabela.Para ver as regras criadas para uma aplicação específica, clique na caixa + ao pé da respectiva aplicação.Limpe a caixa de selecção correspondente a **Ocultar processos de sistema** para poder ver as regras que dizem respeito aos processos de sistema e do BitDefender.

- **Processo/Tipos de Rede** - o processo e os tipos de adaptador de rede aos quais a regra se aplica.As regras são automaticamente criadas para filtrar o acesso à rede ou à Internet através de qualquer adaptador.Pode criar manualmente as regras ou editar as regras existentes para filtrar o acesso à rede ou à Internet de uma aplicação através de um determinado adaptador (por exemplo, um adaptador de rede wireless).
- **Linha de comando** - o comando (**cmd**) usado para iniciar o processo no interface de linha de comando do Windows.

- **Protocolo** - o protocolo IP aos quais as regras se aplicam.Pode ver um dos seguintes:

Protocolo	Descrição
Qualquer	Inclui todos os protocolos IP.
TCP	Transmission Control Protocol - TCP permite que dois hosts estabeleçam uma ligação e troquem dados entre si. O TCP garante a entrega dos dados e também garante que os pacotes serão entregues na mesma ordem em que foram enviados.
UDP	User Datagram Protocol - UDP é um meio de transporte baseado em IP desenhado para uma elevada performance. Os jogos e outras aplicações baseadas em vídeo usam com frequência o UDP.
Um número	Representa um protocolo IP específico (outro que não TCP e UDP).Pode encontrar a lista completa de números IP atribuidos em www.iana.org/assignments/protocol-numbers.

- **Eventos de Rede** - os eventos de rede aos quais a regra se aplica.Os seguintes eventos podem ser tidos em consideração:

Evento	Descrição
Ligar	Intercâmbio preliminar de mensagens standard usado pelos protocolos orientados para a ligação (tais como TCP) para estabelecer a mesma.Com protocolos orientados para a ligação, o tráfego de dados entre dois computadores ocorre apenas após a ligação ser estabelecida.
Tráfego	Fluxo de dados entre dois computadores.
Escutar	Estado em que uma aplicação monitoriza a rede à espera de estabelecer uma ligação ou de receber informação de uma aplicação peer.

- **Portas Locais** - as portas no seu computador em que a regra se aplica.
- **Portas Remotas** - as portas nos computadores remotos em que a regra se aplica.
- **Local** - se a regra só se aplica a computadores na rede local.
- **Acção** -se à aplicação será permitido ou negado o acesso à rede ou Internet nas circunstâncias determinadas.

21.2.2. Adicionar Regras Automaticamente

Com a **Firewall** activada, o BitDefender monitoriza todos as aplicações e cria automaticamente um regra sempre que uma aplicação tenta ligar à Internet.Consoante a aplicação e as definições da firewall doBitDefender, isto é efectuado com ou sem a sua intervenção.

Se estiver a utilizar o Modo Básico ou no Modo Intermédio, as tentativas de ligação de aplicações desconhecidas serão automaticamente bloqueadas.

Se estiver a utilizar o Modo Avançado, ser-lhe-á pedida uma acção, através de uma janela de alerta, sempre que que uma aplicação desconhecida tentar ligar à Internet.

Pode ver o seguinte: a aplicação que se está a tentar ligar à internet, o caminho do ficheiro da aplicação, o destino, o protocolo usado e a porta na qual a aplicação se está a tentar ligar.

Clique **Permitir** para permitir o tráfego (entrada e saída) gerado por esta aplicação a partir do local host para qualquer destino, no respectivo protocolo IP protocol e em todas as portas. Se clicar em **Bloquear**, será negado completamente o acesso à Internet por parte da aplicação no respectivo protocolo IP.

Importante
Permitir tentativas de ligação de entrada apenas de IP's ou domínios em que confia totalmente.

Baseado na sua resposta, uma regra será criada, aplicada e listada na tabela. A próxima vez que a aplicação se tentar ligar, esta regra será aplicada por defeito.

21.2.3. Adicionar Regras Manualmente

A criação manual de regras depende do modo do interface de utilizador.

Modo Intermédio

1. Clique em **Explorar** em **Adicionar Novo Programa**.
2. Localize o programa para o qual pretende criar uma regra e clique em **Abrir**.
3. Clique em **Adicionar regra**.

   Repare que a regra é, agora apresentada na tabela.
4. Seleccione uma acção na coluna **Acção**: permitir ou bloquear o acesso.

   A acção será aplicada a todos os parâmetros da regra.

Modo Avançado

1. Clique no botão **Adicionar Regra** .A janela de configuração irá aparecer.
2. Configure os parâmetros principais e avançados quanto seja necessário.
3. Clique em **OK** para adicionar a nova regra.

As regras só podem ser modificadas durante a configuração da firewall no Modo Avançado.Para modificar uma regra existente, siga os seguintes passos:

1. Clique no botão **Editar Regra** ou faça duplo-clique sobre ela.A janela de configuração irá aparecer.
2. Configure os parâmetros principais e avançados quanto seja necessário.
3. Clique em **Aplicar** para guardar as alterações.

Configurar os Parâmetros Principais

a barra **Principal** da janela de configuração permite configurar os principais parâmetros da regra.

Pode configurar os seguintes parâmetros:

- **Caminho do Programa.** Clique em **Explorar** para seleccionar a aplicação à qual a regra se aplica.Se deseja que a regra se aplique a todas as aplicações, apenas seleccione **Todas**.
- **Linha de comando.** Se deseja que a regra se aplique apenas quando a aplicação é aberta com um comando especifico na linha de comandos do Windows, limpe a caixa **Todas** e insira o respectivo comando no campo de edição.
- **Protocolo.** Seleccione do menu o protocolo IP ao qual a regra se aplica.
  - Se deseja que a regra se aplique a todos os protocolos, seleccione **Todos**.
  - Se deseja que a regra se aplique ao TCP, seleccione **TCP**.
  - Se deseja que a regra se aplique ao UDP, seleccione **UDP**.
  - Se deseja que a regra se aplique a um determinado protocolo, seleccione **Outro**.Um campo de edição irá aparecer.Insira no campo de edição o número atribuido ao protocolo que deseja filtrar.

Nota

Os números dos protocolos IP são atribuidos pelo Internet Assigned Numbers Authority (IANA).Pode encontrar a lista completa de números IP atribuidos em www.iana.org/assignments/protocol-numbers.

- **Eventos.** Dependendo dos protocolo seleccionado, escolha os eventos de rede aos quais a regra se aplica.Os seguintes eventos podem ser tidos em consideração:

Evento	Descrição
Ligar	Intercâmbio preliminar de mensagens standard usado pelos protocolos orientados para a ligação (tais como TCP) para estabelecer a mesma.Com protocolos orientados para a ligação,

Evento	Descrição
	o tráfego de dados entre dois computadores ocorre apenas após a ligação ser estabelecida.
Tráfego	Fluxo de dados entre dois computadores.
Escutar	Estado em que uma aplicação monitoriza a rede à espera de estabelecer uma ligação ou de receber informação de uma aplicação peer.

- **Tipos de Adaptador.** Seleccione os tipos de adaptador a que as regras se aplicam.
- **Acção.** Seleccione uma das seguintes acções disponíveis:

Acção	Descrição
Permitir	À aplicação especificada será permitido o acesso à rede / Internet nas circunstâncias determinadas.
Bloquear	À aplicação especificada será negado o acesso à rede / Internet nas circunstâncias determinadas.

Configurar Parâmetros Avançados

A barra**Avançada** da janela de configuração permite-lhe configurar parâmetros avançados da regra.

Pode configurar os seguintes parâmetros avançados:

- **Direcção.** Seleccione do menu a direcção do tráfego ao qual a regra se aplica.

Direcção	Descrição
Saída	A regra aplica-se apenas ao tráfego de saída.
Entrada	A regra aplica-se apenas ao tráfego de entrada.
Ambos	A regra aplica-se em ambos os sentidos.

- **versão IP.** Seleccione do menu a versão do IP (IPv4, IPv6 ou qualquer) ao qual a regra se aplica.
- **Endereço Local.** Especifique o endereço IP local e a porta aos quais a regra se aplica da seguinte forma:
  - Se tem mais de um adaptador de rede, pode limpar a caixa **Todos** e inserir um endereço IP específico.

- Se escolheu TCP ou UDP como protocolo pode definir uma porta específica ou um range entre 0 e 65535. Se deseja que a regra se aplique a todas as portas seleccione **Todas**.

- **Endereço Remoto.** Especifique o endereço IP remoto e a porta aos quais a regra se aplica da seguinte forma:
  - Para filtrar o tráfego entre o seu computador e um determinado computador, limpe a caixa **Todos** e insira o endereço IP do outro computador.
  - Se escolheu TCP ou UDP como protocolo pode definir uma porta específica ou um range entre 0 e 65535. Se deseja que a regra se aplique a todas as portas seleccione **Todas**.
- **Aplicar esta regra apenas a computadores ligados directamente.** Seleccione esta opção quando deseja que a regra se aplique apenas às tentativas de tráfego locais.
- **Verificar o processo parent chain pelo evento original.** Apenas pode alterar este parâmetro se tiver seleccionado **Regras estritamente automáticas** (vá para a barra Definições e clique **Configuração Avançada**).Regras estritas significa que o BitDefender consulta-o para que tome uma acção quando a aplicação requer acesso à rede/Internet de cada vez que o processo principal é diferente.

21.2.4. Gestão Avançada de Regras

Se precisar de ver e editar as regras que controlam as aplicações com mais pormenor, clique no botão **Avançadas** disponível durante a configuração da firewall no Modo Avançado.

Pode ver as regras da firewall listadas pela ordem em que são verificadas.A tabela de colunas dá-lhe uma informação completa sobre cada regra.

Nota

Quando uma tentativa de ligação é feita (seja de entrada ou saída), o BitDefender aplica a acção da primeira regra que corresponda a essa respectiva ligação.Logo, a ordem pela qual as regras são verificadas é muito importante.

Para eliminar uma regra, seleccione-a e clique no botão **Eliminar Regra**.

Para editar uma regra, seleccione-a e clique no botão **Editar Regra** ou faça duplo-clique sobre ela.

Pode aumentar ou diminuir a prioridade de uma regra. Clique no botão **Subir na Lista** para aumentar um nível a prioridade da regra seleccionada, ou clique no botão **Descer na Lista** para diminuir um nível a prioridade da regra seleccionada.Para atribuir a máxima prioridade a uma regra, clique no botão

Subir Topo. Para atribuir a uma regra a miníma prioridade, clique no botão **Descer Fundo** .

Clique em **Fechar** para fechar a janela.

21.2.5. Apagar e Redifinir Regras

Só é possível eliminar e restaurar regras durante a configuração da firewall no Modo Avançado.

Para apagar uma regra, seleccione-a e clique no botão **Remover regra**.Pode seleccionar e apagar várias regras de uma só vez.

Para eliminar todas as regras criadas para uma especifica aplicação, seleccione-a da lista e clique no botão **Remover regra**.

Se deseja carregar o conjunto de regras por defeito para o nível de confiança seleccionado, clique **Reiniciar Regras**.

21.3. Definições de Rede

Para configurar as definições da ligação de rede, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Segurança** e clique em **Configurar Firewall** na área de Tarefas Rápidas no lado esquerdo da janela. Seleccione o separador **Rede** na nova janela que surge.

Modo Avançado
: Vá a **Firewall > Rede**.

As colunas na tabela **Configuração de Rede** fornecem informações pormenorizadas sobre a rede a que está ligado e permitem configurar as definições da ligação:

- **Adaptador** - o adaptador de rede que o seu computador usa para se ligar à rede ou à Internet.
- **Tipo de Rede** - o tipo de rede a que o adaptador está ligado.Dependendo da configuração do adaptador de rede, o BitDefender pode automaticamente seleccionar um tipo de rede ou solicitar mais informação.

  Altere o tipo clicando na seta na coluna **Tipo de Rede** e seleccionando um dos tipos apresentados na lista.

Tipo de rede	Descrição
Fiável (Mostrar Tudo)	desactiva a firewall para o respectivo dispositivo.

Tipo de rede	Descrição
Casa/Escritório	Permite o tráfego entre o seu computador e os computadores na rede local.
Público	Todo o tráfego é filtrado.
Não Fiável (Bloquear Tudo)	Bloqueia completamente o tráfego de rede e de Internet através do respectivo adaptador.

- **VPN** - se a ligação é ou não VPN (Rede Particular Virtual).

  O tráfego através de ligações VPN é filtrado de forma diferente do tráfego através de outras ligações de rede.Se a ligação for VPN, clique na seta ▾ na coluna **VPN** e seleccione **Sim**.

No Modo Avançado são apresentadas duas colunas adicionais:

- **Stealth** - para não ser detectado por outros computadores.

  Para configurar o Modo Stealth, clique na seta ▾ da coluna **Modo Stealth** e seleccione a opção desejada.

Opção Stealth	Descrição
Em	O Modo Stealth está ligado.O seu computador deixa de ser visível a partir da rede local e da Internet.
Desligado	O Modo Stealth está desligado.Qualquer pessoa da rede local ou da Internet pode fazer ping e detectar o seu computador.
Remoto	O seu computador não pode ser detectado da Internet.As redes locais podem fazer ping e detectar o seu computador.

- **Genérico** - se as regras genéricas são aplicadas a esta ligação.

  Se o endereço IP de um adaptador é alterado, o BitDefender modifica o tipo de rede de acordo com a alteração.Se deseja manter o mesmo tipo, clique na seta ▾ da coluna **Genérico** e seleccione **Sim**.

21.3.1. Zonas de Rede

Pode adicionar computadores autorizados ou bloqueados a uma determinado adaptador.

Uma zona fiável é um computador em que confia totalmente.Todo o tráfego entre o seu computador e o computador fiável é permitido.Para partilhar recursos com

determinados computadores numa rede wireless insegura, adicione-os como computadores autorizados.

Uma zona bloqueada é um computador que você não quer de forma alguma que comunique com o seu.

A tabela **Zonas de Rede** mostra as actuais zonas de rede por adaptador.

Para adicionar uma zona, seleccione o adaptador e clique em **Adicionar Zona**.Uma nova janela irá aparecer.

Proceder da seguinte forma:

1. Seleccione o endereço IP do computador que pretende adicionar.
2. Seleccionar a acção:
   - **Permitir** - para autorizar o tráfego entre o seu computador e o computador seleccionado.
   - **Negar** - para bloquear o tráfego entre o seu computador e o computador seleccionado.
3. Clique em **OK**.

21.4. Dispositivos

Para gerir os dispositivos ligados à rede, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
  Abra o separador **Segurança** e clique em **Configurar a Firewall**, nas Tarefas Rápidas, no lado esquerdo da janela.Seleccione o separador **Dispositivos** na nova janela que aparece.

Modo Avançado
  Vá a **Firewall > Dispositivos**.

Os dispositivos de impressão, fax e digitalização detectados na rede e as respectivas acções predefinidas aparecem na tabela.Para alterar o estado de um dispositivo, faça duplo clique na tabela e seleccione uma acção na janela que aparece: permitir ou bloquear a comunicação com o dispositivo.

Utilize os botões disponibilizados para gerir a lista de dispositivos:

- **Adicionar** - adicionar um dispositivo que não aparece na lista.
- **Remover** - remove um dispositivo seleccionado da lista.
- **Actualizar Dispositivos** - iniciar uma nova análise da rede para actualizar a lista de dispositivos.

21.5. Controlo de Ligação

Para monitorizar a rede actual / actividade na Internet (em TCP e UDP) por aplicação e abrir o registo da Firewall BitDefender, siga os seguintes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Firewall > Actividade**.

Pode ver todo o tráfego por aplicação. Para cada aplicação, pode ver as ligações e as portas abertas, como também as estatísticas com respeito à velocidade de tráfego de saída & entrada e o montante total de dados enviados / recebidos.

Se deseja ver também os processos inactivos, limpe a caixa **Ocultar processos inactivos**.

O significado dos ícones é o seguinte:

- Indica uma ligação de saída.
- Indica uma ligação de entrada.
- Indica uma porta aberta no seu computador.

A janela apresenta em tempo-real a actividade da actual rede / Internet. À medida que as ligações e portas são fechadas, pode ver que as estatísticas correspondentes são diminuidas e que, eventualmente, desaparecerão.A mesma coisa acontece a todas as estatísticas correspondentes a uma aplicação que gera tráfego ou que tem portas abertas que você fecha.

Para obter uma lista mais completa de eventos com respeito ao uso do módulo da Firewall (activar/desactivar a firewall, bloquear tráfego, modificar configurações) ou gerado pelas actividades detectadas por ela (análise de portas, bloqueio de tentativas de ligação ou de tráfego de acordo com as regras) consulte o ficheiro de relatório da Firewall do BitDefender que pode ser visualizado clicando em **Mostrar Relatório**.O ficheiro está localizado na pasta Ficheiros Comuns do actual utilizador do Windows, no caminho: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

Se deseja que o relatório contenha mais informação, seleccione **Aumentar verbosidade do relatório**.

21.6. Resolver Problemas com a Firewall

No caso de encontrar uma incidência que suspeita ser causada pela Firewall do BitDefender, está disponível uma Assistente de Resolução de Problemas para ajudar a resolver.

Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio

Abra o separador **Segurança** e clique em **Configurar a Firewall**, nas Tarefas Rápidas, no lado esquerdo da janela.Seleccione o separador **Definições** na nova janela que aparece e clique em **Resolução de Problemas**.

Modo Avançado

Vá a **Firewall > Definições** e clique em **Resolução de Problemas**.

O assistente pode ajudar a resolver rapidamente os seguintes problemas de conectividade, normalmente associados à configuração da firewall:

- Estou a tentar imprimir e a operação falha.
- Estou a tentar aceder a um computador da minha rede e a operação falha.
- Estou a tentar aceder à Internet e a operação falha.

Se nenhuma das situações descrever o problema que encontrou, seleccione **Outro Problema com a Firewall** para abrir a janela da **Ferramenta de Suporte**.

Para mais informações sobre este assistente, por favor consulte a secção Resolução de Problemas deste manual

22. Vulnerabilidade

Um passo importante na protecção do seu computador contra as pessoas e aplicações maliciosas é manter actualizado o seu sistema operativo e as aplicações que usa regularmente.Mais ainda, para evitar acesso físico não-autorizado ao seu computador, palavras-passe fortes (palavras-passe que não são fáceis de adivinhar) devem de ser criadas para cada conta de utilizador do Windows.

O BitDefender analisa regularmente o seu sistema em busca de vulnerabilidades e notifica-o das incidências existentes.

22.1. A analisar em busca de Vulnerabilidades

Pode verificar as vulnerabilidades e corrigi-las, passo a passo, com o assistente da **Análise de Vulnerabilidade**.Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Segurança** e clique em **Análise de Vulnerabilidade**, nas Tarefas Rápidas, no lado esquerdo da janela.

Modo Avançado
: Vá a **Vulnerabilidade > Estado** e clique em **Verificar Agora**.

Siga o procedimento de seis passos para remover as vulnerabilidades do seu sistema.Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.

1. **Proteja o seu PC**

   Seleccione as vulnerabilidades a verificar.

2. **Analisar incidências seleccionadas...**

   Aguarde que o BitDefender termine a análise de vulnerabilidades ao sistema.

3. **Actualizações do Windows**

   Pode ver a lista das actualizações criticas e não-criticas do Windows que não se encontram actualmente instaladas no seu computador.Seleccione as actualizações que pretende instalar.

4. **Actualizações das Aplicações**

   Se a aplicação não estiver actualizada, clique no link fornecido para descarregar a versão mais recente.

5. **Palavras-passe Fracas**

   Pode ver a lista dos utilizadores de contas Windows configurados no seu computador e o nível de protecção que as suas palavras-passe garantem.Clique em **Reparar** para modificar as palavras-passe fracas.

6. **Sumário**

   Aqui pode ver o resultado da operação.

22.2. Estado

Para ver o estado de vulnerabilidade actual e activar/desactivar a análise de vulnerabilidades automática, siga os seguintes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Vulnerabilidade > Estado**.

A tabela mostrará as incidências que foram encontradas na ultima verificação de vulnerabilidade e o seu estado.Pode ver a acção levada a cabo para reparar cada uma das vulnerabilidades, caso tivesse havido alguma.Se a acção for **Nenhuma**, então a respectiva incidência não representa uma vulnerabilidade.

Importante

Para ser automaticamente notificado acerca das vulnerabilidades do seu sistema e aplicações, mantenha a **Análise Automática de Vulnerabilidades** activada.

Dependendo da incidencia, para reparar uma vulnerabilidade específica proceda da seguinte forma:

- Se estiverem disponiveis actualizações do Windows, clique em **Instalar** na coluna **Acções** para as instalar.
- Se uma aplicação estiver desactualizada, clique em **Mais informações** para saber a versão e seguir a hiperligação para a página de Internet do fornecedor a partir da qual pode instalar a versão mais recente dessa aplicação.
- Se uma conta de utilizador do Windows tem uma palavra-passe fraca, clique em **Ver & Corrigir**a para forçar o utilizador a mudar a palavra-passe da próxima vez que entrar no Windows ou então mude a palavra-passe directamente.Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).
- Se o recurso Execução Automática estiver activado no Windows, clique em **Corrigir** para o desactivar.

22.3. Definições

Para configurar as definições da verificação de vulnerabilidade automática, siga os seguintes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Vulnerabilidade > Definições**.

3. Seleccione as caixas que correspondem às vulnerabilidades do sistema que deseja que sejam regularmente verificadas.
   - **Actualizações Críticas do Windows**
   - **Actualizações Regulares do Windows**
   - **Actualizações das Aplicações**
   - **Palavras-passe Fracas**
   - **Execução Automática**

Nota

Se limpar a a caixa correspondente a uma determinada vulnerabilidade, o BitDefender não o irá mais notificar acerca das incidências relacionadas.

23. Backup

BitDefender vem com um módulo de Backup que o ajuda a fazer cópias de reserva de todos os dados valiosos no seu sistema. Pode fazer backup para o seu computador, discos amovíveis ou para uma localização de rede para se certificar que os pode restaurar quando necessário. O restauro dos seus dados é um processo muito fácil.

As seguintes tarefas ajudam a fazer backup e a restaurar os seus dados:

- Backup Local - um procedimento de cinco passos para fazer um backup dos seus dados localmente.
- Restauro Local - um procedimento de quatro passos para restaurar os seus dados localmente.

Pode configurar e executar operações de backup nas Definições do Backup BitDefender.

23.1. Fazer o Backup Local de Dados

O Assistente de Backup Local vai orientar o processo de criação de uma tarefa de backup local. No final do processo será capaz de fazer backup dos seus dados na hora ou agendar o produto para o fazer mais tarde.

Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: No separador **Armazenamento de Ficheiros**, clique em **Backup Local** na área de Tarefas Rápidas no lado esquerdo da janela e seleccione Backup Local.

Modo Avançado
: Vá a **Backup** e clique em **Backup Local**.

Nota
Também pode adicionar um atalho a Meus Instrumentos.

Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Janela de boas-vindas**
2. **Escolha o que deseja fazer Backup**

   Pode escolher fazer **Backup Rápido** (a sua música, videos, imagens, e-mails, definições de aplicações, etc.) ou **Backup Completo** (todas as partições).

   Clique em **Outros ficheiros**, para adicionar outros ficheiros do seu Ambiente de Trabalho ao **Backup Rápido**. O **Backup Completo** pode também ser

facilmente personalizado ao seleccionar que directórios de um determinada partição deseja fazer backup.

3. **Escolha onde guardar o Backup**

   Aqui pode seleccionar o local onde guardar os dados do backup.

   Se decidir fazer backup para o seu computador, a sua drive USB ou num local de rede, clique em **Escolher Local** e seleccione o local onde deseja guardar os dados.

   Se deseja fazer backup dos seus dados para o servidor FTP, clique em **Escolher Local** e adicione o servidor FTP.Uma nova janela irá aparecer.

   Deve de configurar as definições de ligação ao servidor FTP da seguinte forma:
   a. Insira o nome do servidor FTP no campo correspondente.
   b. Se o servidor FTP usa uma porta diferente da porta 12 por defeito insira-a no campo correspondente.
   c. Para usar o modo passivo (O servidor FTP inicia a ligação), marque a caixa **Modo Passivo**.
   d. Se o servidor FTP permite o acesso anónimo, pode deixar a opção **Anónimo** seleccionada.De outra forma, seleccione**Nome de Utilizador** e introduza o nome de utilizador e a palavra-passe reconhecida pelo servidor FTP.
   e. Clique em **OK**.

4. **Escolher quando fazer o Backup**

   Aqui pode seleccionar quando deseja fazer o backup dos dados.

   Para fazer backup dos ficheiros na hora clique em **Fazer Backup dos dados só esta vez**, para agendar o produto para fazer backup mais tarde, clique **Fazer Backup dos dados numa data agendada por mim**.

   Se seleccionar **Fazer Backup dos dados numa data agendada por mim**, pode especificar com que frequência a tarefa agendada será executada: diariamente ou semanalmente. Pode também especificar a data e a hora.

5. **Sumário**

   Aqui pode rever as definições da tarefa de backup e dar início ao mesmo.

   Deve inserir um nome de tarefa no campo correspondente.

   Clique em **Iniciar backup** se estiver satisfeito com as suas definições.Aguarde que o BitDefender complete o backup e clique em **Terminar**.

Nota

Da primeira vez que criar uma tarefa de backup agendada, será notificado para especificar a conta do Windows a usar para executar a tarefa.

Para usar a actual conta, apenas insira a sua palavra-passe no campo correspondente.Se deseja levar a cabo o backup sob uma conta diferente, seleccione **O seguinte utilizador Windows** e preencha os campos.

- **Nome de Utilizador** - insira o nome da conta do Windows.
- **Palavra-passe** - insira a palavra-passe do utilizador previamente definido.
- **Servidor** - insira o nome do servidor de domínio.

Clique em **OK** para continuar.

23.2. Restaurar Dados de Backup Local

O Assistente de Restauro Local ajuda-o a restaurar os dados guardados no meio de armazenamento local. No final do processo será capaz de fazer backup dos seus dados na hora ou agendar o produto para o fazer mais tarde.

Nota

Antes de restaurar quaisquer dados, assegure-se que o dispositivo onde se encontram os mesmos se encontra disponível.Dependendo do dispositivo que utiliza, poderá necessitar de levar a cabo uma das seguintes acções:

- Inserir a pen USB do backup na porta USB.
- Inserir o CD/DVD do backup na respectiva drive.
- Verifique que é possível ligar-se ao local da rede ou ao servidor FTP onde se encontra armazenado o backup.

Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: No separador **Armazenamento de Ficheiros**, clique em **Backup Local** na área de Tarefas Rápidas no lado esquerdo da janela e seleccione Restauro Local.

Modo Avançado
: Vá a **Backup** e clique em **Restauro Local**.

Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Janela de boas-vindas**
2. **Escolha do que fazer Backup**

   Aqui pode seleccionar um local de onde deseja restaurar os ficheiros.

   Após seleccionar uma opção, clique em **Escolher Local** e seleccione o ficheiro de backup que deseja restaurar.
3. **Escolher o Local e os Ficheiros de Restauro**

   Aqui é onde pode escolher que ficheiros específicos a restaurar e para onde os restaurar.

   Se deseja restaurar dados para outro local ou apenas ficheiros específicos, seleccione o local e os dados clicando no botão correspondente.

Para evitar sobreescrever o ficheiro existente durante o restauro, limpe a caixa de selecção **Sobrescrever os ficheiros existentes quando restaurar**.

4. **Sumário**

   Aqui pode rever as definições da tarefa de restauro e dar início ao mesmo.

   Clique em **Restaurar** se estiver satisfeito com as suas definições.Aguarde que o BitDefender restaure os dados seleccionados e depois clique em **Terminar**.

23.3. Definições de Backup

Se necessita de levar a cabo uma operação de backup e restauro mais complexa, pode usar a solução do BitDefender Backup com todas as opções.O Backup BitDefender oferece:

- uma variedade de opções de backup, tais como compressão, encriptação, e filtragem de ficheiros para backup ou definir a velocidade de backup.
- controlo refinado no restauro de ficheiros (por exemplo, pode restaurar dados dos quais fez um backup num determinado ponto do tempo).
- capacidade de agendamento avançada (por exemplo, pode escolher iniciar o seu backup durante o arranque do sistema ou quando o computador estiver ianctivo).
- um visualizador de relatório que o ajuda a manter um registo das operações de backup e restauro que levou a cabo e assim reparar eventuais erros.

Para abrir o Backup do BitDefender, siga os seguintes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Backup** e clique em **Definições** .

Existem duas formas como pode estabelecer e executar operações de backup. Ou acede à **Barra de Menu** superior, ou clica numa determinada barra a partir da **Barra de Navegação**.

A **Barra de Navegação**, mostrada na parte superior da janela principal e por debaixo da **Barra de Menu**, dá acesso a quatro secções:

- **Iniciação**
- **Admin de Tarefas**
- **Visualizador de Relatórios**
- **Caixa de Ferramentas**

23.3.1. Iniciação

A área de **Introdução** ajuda-o a fazer facilmente backups dos seus e-mails, registos de chat e dados.

Pode mudar para a **Introdução** fazendo o seguinte:

- Clique em **Introdução** na **Barra de Navegação**.
- Clique em **Ver** na **Barra de Menu** e seleccione **Introdução**.
- Use um atalho premindo as teclas **CTRL+Alt+S**.

Para fazer backup dos seus documentos chave, fotos, e-mails e registos de chat durante a mesma tarefa, clique no botão **Fazer Backup Dados** e siga o procedimento de três passos.

Para fazer backup apenas dos seus e-mails clique no botão **Fazer Backup E-mails** e siga o procedimento de três passos.

Para fazer backup apenas dos seus registos de chat, clique no botão **Fazer Backup do Chat** e siga o procedimento de três passos.

Nota
O procedimento de tres passos está descrito na secção“*Criar Nova Tarefa*” (p. 153).

23.3.2. Admin de Tarefas

Gestor de Tarefa é usado para ver e gerir tarefas de backup, ver proprieddes das tarefas e os relatórios das tarefas como também monitorizar a velocidade de execução da mesma. **Gestor de Tarefa** permite verificar as propriedades da tarefa e o seu estado actual, modificando as definições da tarefas como também executando a tarefa de backup ou restauro.

Pode mudar para o **Gestor de Tarefa** fazendo o seguinte:

- Clique em **Gestor de Tarefa** na **Barra de Navegação**.
- Clique em **Ver** na **Barra de Menu** e seleccione **Gestor de Tarefa**.
- Use um atalho premindo as teclas **CTRL+Alt+M**.

À esquerda, poderá ver uma lista de links de operações rápidas, como se seguem:

Administração de Tarefas
- **Criar Nova Tarefa**
- **Tarefa de Backup**
- **Tarefa Agendada**
- **Apagar Tarefa Agendada**
- **Mudar Opções de Tarefa**
- **Mudar Propriedades Tarefa**

Restauro de Tarefas
- **Restaurar Ficheiro**
- **Restaurar Time-Point Data**

Controlo de Tarefas
- **Pausa na Tarefa**
- **Parar Tarefa**
- **Parar Tudo**

Criar Nova Tarefa

Para fazer backup dos seus documentos chave, fotos, e-mails e registos de chat durante a mesma tarefa, clique no botão**Criar Nova Tarefa** e siga os próximos três passos.

1. Clique na caixa de selecção para selecionar partições, directórios, ou ficheiros para backup.

   Quando selecciona um item no lado esquerdo da janela, o seu conteúdo será mostrado no lado direito da janela para o ajudar a refinar a sua selecção.
2. Insira um nome para a sua tarefa de backup ou aceite o nome por defeito da mesma.

   O nome por defeito da tarefa é automaticamente gerado quando os ficheiros ou os directórios são seleccionados para serem backup, mas pode ser modificado.
3. Clique em **Explorar** para escolher onde guardar a sua tarefa de backup.

Nota
Não se esqueça de clicar em **Backup** para iniciar ou **Cancelar** para parar.
Para refinar as suas definições, clique em **Opções**.

Caixa de Diálogo Opções de Backup

Existem diversas sub-opções na caixa de diálogo das **Opções**.

Tipo de Backup

O Backup BitDefender suporta dois tipos de backup.

- **Backup Total:** Faz um backup completo de fonte de dados seleccionada para o backup set no destino especificado. Quando executar um backup total, o Backup BitDefender não fará backup dos dados modificados mas sim de toda a fonte de dados.
- **Backup Incremental:** Quando executar pela primeira o Backup Incremental é o mesmo que o Backup Total porque faz um backup completo de toda a fonte de dados para o backup set no destino especificado. Mais tarde, apenas faz backup dos novos ficheiros ou dos ficheiros modificados. Sempre que um Backup Incremental Backup é executado um backup catalog set é criado.

O Backup Incremental e o Total podem também combinar-se num **Backup de Rotação**. Por exemplo, pode definir um Backup Incremental do trabalho enquanto definie um Backup Total uma vez por semana, digamos ao Domingo. Eis como é feito: Seleccione **Semanal** do menu drop-down, 1 do campo**Cada Semana** e seleccionar Domingo. Este Backup Total ao Domingo substituirá todos os backups anteriores e será a base para o novo Backup Incremental trabalhar.

Conjunto de Catálogo

É usado para indexar toda a informação de ficheiros de cada backup, e é a base do processos de Backup Incremental e Restauração. O catalog set (`*.ecs`) contém uma série de catálogos que representam um índice de todos os ficheiros e directórios existente no backup set. Tal índice inclui os dados da data do backup, directório de backup, nome do ficheiro e propriedades. Os dados podem ser restaurados a partir do catalog set.

Um nome de ficheiro de catalog set é gerado automaticamente por destino de tarefa. Para modificar o catalog set de uma tarefa faça o seguinte:

1. Clique em **Catalog Set**.
2. Insira um nome de ficheiro no campo correspondente.
3. Clique em **Explorar** para seleccionar o directório onde guardar os ficheiros do Catalog set.
4. Clique em **OK**.

Compressão de Dados

O Backup BitDefender permite a comprimir e guardar os dados para o backup set quando executa um backup para poupar espaço. Suporta Compressão Rápida, Compressão Standard, Compressão Alta Intensidade. Por exemplo, para iniciar a compressão standard a uma velocidade de compressão média, siga os seguintes passos:

1. Clique em **Compressão de Dados**.
2. Clique em **Compressão Standard**.
3. Clique em **OK**.

Espaço de Destino

O Backup BitDefender permite a distribuição do backup set para um destino diferente. neste caso, mesmo que um determinado destino não tenha suficiente espaço livre, a execução do backup dos dados prosseguirá.

Pode adicionar um ou mais destinos para continuar o backup, modificá-lo ou mesmo removê-lo, da seguinte forma:

1. Clique em **Span de Destino**.
2. Clique em **Adicionar** para seleccionar um novo destino para guardar os dados de backup..
3. Clique em **Editar** para modificar o destino de backup seleccionado.
4. Clique em **Apagar** para apagar o destino de backup seleccionado.
5. Clique em **Apagar Todos** para apagar todos os destinos de backup.
6. Clique em **OK**.

Encriptação

O Backup BitDefender mantém os dados backup mais seguros ao encriptá-los antes de os guardar no backup set. As definições de segurança de uma tarefa inclui protecção por palavra-passe.

Para encriptar os dados antes do backup, siga estes passos:

1. Clique em **Encriptação**.

2. Seleccione um tipo de encriptação a partir do menu drop-down.
3. Insira a sua palavra-passe no campo correspondente.
4. Reinsira a sua palavra-passe no campo correspondente.
5. Clique em **OK**.

Programa Externo

A tarefa pode executar outro comando antes ou depois do backup, e o comando pode ser `.exe`, `.com` ou `.bat`, ou um tipo específico de evento tal como "desligar o computador após terminar o backup".

Para executar o comando quando o backup inicia, siga os seguintes passos:
1. Clique em **Programa Externo**
2. Seleccione a opção**Antes da Execução da Tarefa** .
3. Clique em **Explorar** para seleccionar os ficheiros de comando a executar.
4. Clique em **OK**.

Para executar o comando após o backup ter terminado, siga estes passos:
1. Clique em **Programa Externo**
2. Seleccione a opção **Executar Após Tarefa** .
3. Clique em **Explorar** para seleccionar os ficheiros de comando a executar.
4. Ou clique em **Desligar o PC** quando o backup terminar.
5. Ou clique em **Reiniciar o PC** quando o backup terminar.
6. Ou clique em **Sair do utilizador actual** quando o backup terminar.
7. Clique em **OK**.

Nota

Se deseja que a configuração funcione mesmo em caso de falha do backup, marque a caixa de selecção **Executar Aplicação Externa mesmo que a execução da tarefa falhe**.

Filtro de Ficheiro

O Backup BitDefender fornece uma função de filtragem poderosa para excluir ou incluir ficheiros específicos, tipos de ficheiros ou directórios, para poupar espaço de armazenamento e melhorar a velocidade de backup.

Tipos de ficheiros especifoicados podem ser filtrados, seguindo os seguintes passos:
1. Clique em**Filtro de Ficheiros**.
2. Clique em **Tipo de Filtro**.
3. Exclui ou inclui tipos de ficheiros nos pop-ups das caixas de diálogo ao seleccionar as opções **Incluir apenas tipos de ficheiros seleccionados** ou **Excluir tipos de ficheiros seleccionados** .
4. Se necessário, insira outro tipo de ficheiro no campo **Tipo Personalizado** mas assegure-se de usar o formato `.abc` . Use a `,` (virgula) como separador quando inserir mais do que um tipo personalizado. Adicione uma breve descripção no campo correspondente.
5. Clique em **OK**.

Um ficheiro especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique em **Filtrar Ficheiro**.
3. Exclua ou inclua ficheiros específicos nos pop-ups das caixas de diálogo seleccionando as opções **Incluir apenas os ficheiros especificados por regra** ou **Excluir os ficheiros especificados** .
4. Clique em **Explorar** e seleccione o ficheiro. O caminho da localização do ficheiro será automaticamente adicionado no campo **Aplicar aos seguintes directórios** . Para incluir ou excluir o respectivo ficheiro da sua localização, clique em **Aplicar a todos os directórios**.
5. Clique em **OK**.

O directório especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique em **Filtrar Directório**.
3. Exclui ou inclui directórios específicos nos pop-ups das caixas de diálogo ao seleccionar as opções **Incluir apenas os directórios especificados por regra** ou **Excluir os directórios especificados por regra** .
4. Clique em **Explorar** e seleccione o directório. O caminho para o local do directório será automaticamente adicionado no campo **Aplicar aos seguintes directórios** . Para incluir ou excluir respectivos directórios do seu local, clique em **Aplicar a todos os directórios**.
5. Clique em **OK**.

Os filtros podem ser modificados seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique no filtro que deseja modificar e clique em **Editar**.
3. Modifique as suas opções na caixa de diálogo.
4. Clique em **OK**.

Os filtros podem ser apagados seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique no filtro que deseja remover e clique em **Apagar**.
3. Ou clique **Apagar Todos** directamente, para apagar todos os filtros.
4. Clique em **OK**.

Transferência de Rede

O Backup BitDefender permite fazer backup e restaurar dados partilhados em grupos de trabalho de rede minuciosamente. Se a rede não estiver acessível, tentará fazer backup dos dados de vez em quando. Para especificar com que frequência ou quantas vezes deseja tentar o backup, siga os seguintes passos:

1. Clique em **Transferência de Rede**.
2. Clique em **Quando falhar em ler ficheiros de rede devido a desconexão, tentar conectar de novo**.
3. Insira com que frequência deseja tentar de novo o backup dos dados (em segundos).

4. Insira quantas vezes deseja tentar de novo o backup dos dados.
5. Clique em **OK**.

Nota

Para evitar ser esmagado por informação de erros de rede, clique em **Não é gerado relatório de erro quando a rede não está disponível**.

Dividir conjunto de backup

O backup set gerado pode ser dividido emdiveros outros backup sets, de forma a que o backup possa ser executado normalmente mesmo quando o destino ou o sistema de ficheiros é limitado. O Backup BitDefender dá-lhe dois métodos de divisão: auto-divisão e divisão-definida.

As definições de divisão da tarefa de backup podem ser modificadas da seguinte forma:

1. Clique em **Dividir Backup Set**.
2. Seleccionar **Divisão Automática por Espaço no Destino**.
3. Ou seleccione **Especificar tamanho para dividir** e escolha o tamanho desejado no menu drop down.
4. Clique em **OK**.

Velocidade

O Backup BitDefender suporta três tipos de velocidade. Quanto maior a velocidade, mais CPU será ocupado.

A velocidade de Backup pode ser especificada seguindo estes passos.

1. Clique em **Velocidade**.
2. Seleccione velocidade**Rápida**, **Média** ou **Baixa** .
3. Clique em **OK**.

Verificação de Dados

Para ter a certeza de que os seus dados de backup estão sempre seguros, siga este passos:

1. Clique em **Verificação de Dados**.
2. Clique em **Verificar os dados no processo de backup**.
3. Clique em **OK**.

Tarefa de Backup

Uma vez que a tarefa tenha sido criada, o backup é executado automaticamente. No entanto, pode entrar em **Gestor de Tarefa** para executar backup ao seleccionar a tarefa criada e clicar no menu **Tarefa de Backup** .

De forma a receber os detalhes do backup quando restaurar os ficheiros, deve de inserir uma breve descripção na janela de pop-up que se abre. Clique em **Cancelar** para ignorar a janela de pop-up ou **OK** para continuar. A tarefa de backup pode ser cancelada ao clicar no botão **Cancelar Backup** .

Nota

Para informação detalhada, uma boa ideia seria ver as **Propriedades**, **Relatórios** e **Info Execução** da tarefa a partir da janela da barra de estado.

Agendar Tarefa

Aqui é onde poderá agendar a tarefa de backup para uma altura que seja conveniente. Pode agendar a tarefa para ser executada diariamente, semanalmente, mensalmente ou a qualquer altura que deseje (por exemplo durante o arranque do sistema). **Agendar Tarefa** é a base para o backup automático.

Se o seu computador é membro de um domínio de rede, uma série de passos extra são necessários para agendar uma tarefa.

1. Seleccione a tarefa e depois clique em **Agendar Tarefa**.
2. A caixa de diálogo de **Utilizador de Execução** aparecerá. Se é um utilizador do domínio, por favor insira a palavra-passe do domínio.
3. De outra forma seleccione **Executar como o seguinte utilizador Windows**.
4. Insira o nome do utilizador, palavra-passe e o nome do servidor de domínio.
5. Clique em **OK**.

Uma vez que defina o utilizador de execução, o Backup BitDefender mostrará a caixa de diálogo **Agendar** de forma a que possa definir uma altura conveniente para executar a tarefa.

É aqui onde pode especificar a frequência com que as tarefas agendadas se executam: diariamente, semanalmente, mensalmente, uma vez, no arranque do sistema, no login, quando o computador está em descanso. Se a tarefa é agendada diariamente, semanalmente, mensalmente, uma só vez, pode também especificar a hora de início. Pode também seleccionar com que frequência a tarefa agendada é executada (expresso como o número de dias ou semanas, o dia do mês ou a data). Outra definição possível é a duração (em minutos) do período de descanso após o qual a tarefa agendada se inicia.

É também possível configurar múltiplos agendamentos para uma tarefa clicando em **Mostrar múltiplos agendamentos**. Ao clicar **Avançado** pode definir opções adicionais de agendamento. Por exemplo, pode definir a data de início e fim da tarefa.

Para refinar ainda mais a tarefa agendada, clique na barra **Definições** . Três sub-opções estão disponíveis.

- **Tarefa Agendada Terminada**
  - Apague a tarefa se não estiver agendada para se executar novamente.

    Esta tarefa é útil para tarefas agendadas para se executarem uma só vez.
  - Parar a tarefa se se executa para:

    Especifique por quanto tempo após a tarefa ter sido iniciada deverá ser parada.
- **Tempo de Descanso**

- Apenas inicia a tarefa se o computador estiver em descanso há pelo menos:

  Especifique quanto tempo (em minutos) deve passar sem usar o rato ou o teclado antes de a tarefa agendada se iniciar.
- Se o computador não estiver estado em descanso tanto tempo, tentar de novo com:

  Especifique quanto tempo (em minutos) a tarefa deve continuar a verificar se o computador está em descanso.
- Parar a tarefa se o computador deixar de estar em descanso.

  Especifique se a tarefa deve ser parada se você começar a usar o computador enquanto a tarefa estive a decorrer.

● **Gestor de Energia**

- Não inicie a tarefa se o seu computador estiver a funcionar a bateria.

  Especifique se a tarefa deve ser impedida de inciar enquanto o seu computador está a funcionar a bateria. Ao seleccionar esta caixa de selecção pode aumentar a duração da sua bateria.
- Parar a tarefa se o modo de bateria iniciar.

  Especifique se a tarefa deve ser parada quando o seu computador começar a funcionar a bateria.
- Desperte o computador para executar esta tarefa.

  Especifica se o computador deve executar a tarefa agendada mesmo que esteja no modo de Hibernação.

Apagar Tarefa Agendada

Para apagar uma tarefa agendada, seleccione-a e clique em**Apagar Tarefa Agendada** na secção**Gestão de Tarefas** .

Se a tarefa não está agendada, **Apagar Tarefa Agendada** será mostrada a cinzento, significando que não é usada.

Mudar Opções de Tarefa

Para modificar opções da tarefa, seleccione-a e clique em **Modificar Opções da Tarefa** na secção **Gestão de Tarefas** .

A tarefa selecionada pode ser uma tarefa de backup ou uma gravação.

Para mais informação sobre a modificação de tarefas de backup, consulte o *“Caixa de Diálogo Opções de Backup”* (p. 153).

Vamos ver como podem ser modificadas as tarefas de gravação.

Modificar Opções da Tarefa de Gravação

Várias sub-opções estão disponíveis na caixa de diálogo da tarefa de gravação.

Gravar

Aqui é onde pode definir que o disco seja ejectado após a gravação ter terminado (se deseja partilha-lo com outros) ou escrito usando o ficheiro de sistema Joliet (menos restrições no nome do ficheiro).

Se deseja agendar a tarefa, clique em **Definir Agendar**.

Aqui é onde poderá agendar a tarefa de backup para uma altura que seja conveniente. Pode agendar a tarefa para ser executada diariamente, semanalmente, mensalmente ou a qualquer altura que deseje (por exemplo durante o arranque do sistema). **Agendar Tarefa** é a base para o backup automático.

Se o seu computador é membro de um domínio de rede, uma série de passos extra são necessários para agendar uma tarefa.

1. Seleccione a tarefa e depois clique em **Agendar Tarefa**.
2. A caixa de diálogo de **Utilizador de Execução** aparecerá. Se é um utilizador do domínio, por favor insira a palavra-passe do domínio.
3. De outra forma seleccione **Executar como o seguinte utilizador Windows**.
4. Insira o nome do utilizador, palavra-passe e o nome do servidor de domínio.
5. Clique em **OK**.

Uma vez que defina o utilizador de execução, o Backup BitDefender mostrará a caixa de diálogo **Agendar** de forma a que possa definir uma altura conveniente para executar a tarefa.

É aqui onde pode especificar a frequência com que as tarefas agendadas se executam: diariamente, semanalmente, mensalmente, uma vez, no arranque do sistema, no login, quando o computador está em descanso. Se a tarefa é agendada diariamente, semanalmente, mensalmente, uma só vez, pode também especificar a hora de início. Pode também seleccionar com que frequência a tarefa agendada é executada (expresso como o número de dias ou semanas, o dia do mês ou a data). Outra definição possível é a duração (em minutos) do período de descanso após o qual a tarefa agendada se inicia.

É também possível configurar múltiplos agendamentos para uma tarefa clicando em **Mostrar múltiplos agendamentos**. Ao clicar **Avançado** pode definir opções adicionais de agendamento. Por exemplo, pode definir a data de início e fim da tarefa.

Para refinar ainda mais a tarefa agendada, clique na barra **Definições** . Três sub-opções estão disponíveis.

- **Tarefa Agendada Terminada**
  - Apague a tarefa se não estiver agendada para se executar novamente.

    Esta tarefa é útil para tarefas agendadas para se executarem uma só vez.
  - Parar a tarefa se se executa para:

Especifique por quanto tempo após a tarefa ter sido iniciada deverá ser parada.

- **Tempo de Descanso**
  - Apenas inicia a tarefa se o computador estiver em descanso há pelo menos:

    Especifique quanto tempo (em minutos) deve passar sem usar o rato ou o teclado antes de a tarefa agendada se iniciar.
  - Se o computador não estiver estado em descanso tanto tempo, tentar de novo com:

    Especifique quanto tempo (em minutos) a tarefa deve continuar a verificar se o computador está em descanso.
  - Parar a tarefa se o computador deixar de estar em descanso.

    Especifique se a tarefa deve ser parada se você começar a usar o computador enquanto a tarefa estive a decorrer.
- **Gestor de Energia**
  - Não inicie a tarefa se o seu computador estiver a funcionar a bateria.

    Especifique se a tarefa deve ser impedida de inciar enquanto o seu computador está a funcionar a bateria. Ao seleccionar esta caixa de selecção pode aumentar a duração da sua bateria.
  - Parar a tarefa se o modo de bateria iniciar.

    Especifique se a tarefa deve ser parada quando o seu computador começar a funcionar a bateria.
  - Desperte o computador para executar esta tarefa.

    Especifica se o computador deve executar a tarefa agendada mesmo que esteja no modo de Hibernação.

Programa Externo

A tarefa pode executar outro comando antes ou depois do backup, e o comando pode ser `.exe`, `.com` ou `.bat`, ou um tipo específico de evento tal como "desligar o computador após terminar o backup".

Para executar o comando quando o backup inicia, siga os seguintes passos:
1. Clique em **Programa Externo**
2. Seleccione a opção**Antes da Execução da Tarefa** .
3. Clique em **Explorar** para seleccionar os ficheiros de comando a executar.
4. Clique em **OK**.

Para executar o comando após o backup ter terminado, siga estes passos:
1. Clique em **Programa Externo**
2. Seleccione a opção **Executar Após Tarefa** .
3. Clique em **Explorar** para seleccionar os ficheiros de comando a executar.
4. Ou clique em **Desligar o PC** quando o backup terminar.
5. Ou clique em **Reiniciar o PC** quando o backup terminar.
6. Ou clique em **Sair do utilizador actual** quando o backup terminar.

7. Clique em **OK**.

Nota

Se deseja que a configuração funcione mesmo em caso de falha do backup, marque a caixa de selecção **Executar Aplicação Externa mesmo que a execução da tarefa falhe**.

Filtro de Ficheiro

O Backup BitDefender fornece uma função de filtragem poderosa para excluir ou incluir ficheiros específicos, tipos de ficheiros ou directórios, para poupar espaço de armazenamento e melhorar a velocidade de backup.

Tipos de ficheiros especifoicados podem ser filtrados, seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique em **Tipo de Filtro**.
3. Exclui ou inclui tipos de ficheiros nos pop-ups das caixas de diálogo ao seleccionar as opções **Incluir apenas tipos de ficheiros seleccionados** ou **Excluir tipos de ficheiros seleccionados** .
4. Se necessário, insira outro tipo de ficheiro no campo **Tipo Personalizado** mas assegure-se de usar o formato **.abc** . Use a **,** (virgula) como separador quando inserir mais do que um tipo personalizado. Adicione uma breve descripção no campo correspondente.
5. Clique em **OK**.

Um ficheiro especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique em **Filtrar Ficheiro**.
3. Exclua ou inclua ficheiros específicos nos pop-ups das caixas de diálogo seleccionando as opções **Incluir apenas os ficheiros especificados por regra** ou **Excluir os ficheiros especificados** .
4. Clique em **Explorar** e seleccione o ficheiro. O caminho da localização do ficheiro será automaticamente adicionado no campo **Aplicar aos seguintes directórios** . Para incluir ou excluir o respectivo ficheiro da sua localização, clique em **Aplicar a todos os directórios**.
5. Clique em **OK**.

O directório especificado pode ser filtrado seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique em **Filtrar Directório**.
3. Exclui ou inclui directórios específicos nos pop-ups das caixas de diálogo ao seleccionar as opções **Incluir apenas os directórios especificados por regra** ou **Excluir os directórios especificados por regra** .
4. Clique em **Explorar** e seleccione o directório. O caminho para o local do directório será automaticamente adicionado no campo **Aplicar aos**

seguintes directórios . Para incluir ou excluir respectivos directórios do seu local, clique em **Aplicar a todos os directórios**.

5. Clique em **OK**.

Os filtros podem ser modificados seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique no filtro que deseja modificar e clique em **Editar**.
3. Modifique as suas opções na caixa de diálogo.
4. Clique em **OK**.

Os filtros podem ser apagados seguindo os seguintes passos:

1. Clique em**Filtro de Ficheiros**.
2. Clique no filtro que deseja remover e clique em **Apagar**.
3. Ou clique **Apagar Todos** directamente, para apagar todos os filtros.
4. Clique em **OK**.

Verificação de Dados

Para ter a certeza de que os seus dados de backup estão sempre seguros, siga este passos:

1. Clique em **Verificação de Dados**.
2. Clique em **Verificar os dados no processo de backup**.
3. Clique em **OK**.

Mudar Propriedades Tarefa

Para modificar as propriedades da tarefa, seleccione a tarefa em questão e depois clique em **Modificar Propriedades da Tarefa** na secção **Gestão de Tarefa**.

1. Clique na caixa de selecção para selecionar partições, directórios, ou ficheiros para backup.

   Quando selecciona um item no lado esquerdo da janela, o seu conteúdo será mostrado no lado direito da janela para o ajudar a refinar a sua selecção.
2. Insira um nome para a sua tarefa de backup ou aceite o nome por defeito da mesma.

   O nome por defeito da tarefa é automaticamente gerado quando os ficheiros ou os directórios são seleccionados para serem backup, mas pode ser modificado.
3. Clique em **Explorar** para escolher onde guardar a sua tarefa de backup.

Nota

Não se esqueça de clicar em **Backup** para iniciar ou **Cancelar** para parar. Para refinar as suas definições, clique em **Opções**.

Restaurar Ficheiro

Para restaurar o backup dos seus dados, seleccione a tarefa da qual deseja restaurar os dados, e clique em **Restaurar Ficheiro** no menu **Restaurar Tarefa** e depois siga estes passos.

1. Selecciones as caixas de selcção perto das partições, directórios, ou ficheiros seleccionados para serem restaurados.

   Quando selecciona um item no lado esquerdo da janela, o seu conteúdo é mostrado no lado direito da janela para o ajudar a refinar a sua selecção.
2. Na janela **Seleccionar Local de Restauro**, pode usar o local original sem quaisquer mudanças, ou especificar outro local para onde restaurar o ficheiro.

   Clique em **Explorar** para escolher onde guardar a sua tarefa de backup.

Nota
Não se esqueça de clicar em **Restaurar** para iniciar ou **Cancelar** para parar. Para refinar as suas definições, clique em **Opções**.

Caixa de Diálogo Opções de Restaurar

As opções de restaurar permitem especificar se os ficheiros a serem restaurados já existem no destino na altura do restauro em si, e se actualiza a data modificada de cada ficheiro restaurado.

Quando os ficheiros a restaurar já existem

- **Ignorar Ficheiros** O BitDefender ignora os ficheiros respectivos.
- **Pergunta ao utilizador se deseja ou nao substituir o Ficheiro** O BitDefender pergunta se deve ou não substituir os ficheiros
- **Substituir Directo** O BitDefender substitui os ficheiros sem perguntar.
- **Substituir Antigos** O BitDefender substitui apenas os ficheiros antigos. Os ficheiros antigos são determinados baseado na data em que foram modificados.

Data de Modificação do Ficheiro

Se a opção for seleccionada, o BitDefender usa a data actual para indicar a data em que os ficheiros ou directórios foram restaurados. Se não, o BitDefender usa a data de modificação do ficheiro ou directório de quando foi feito o backup.

Estrutura de Directório

Só se torna activa quando escolhe outro local para onde restaurar os dados. Pode também preservar a estrutura de directório dos seus dados.

Restaurar Time-Point Data

Para restaurar os dados de um backup de um determinado ponto do tempo, selecciona a tarefa da qual deseja restaurar os dados, e clique em **Restaurar Dados do Ponto do Tempo** no menu **Restaurar Tarefa** e então siga os seguintes passos.

1. Seleccione o backup set de um determinado ponto do tempo da lista. Comentários serão mostrados por debaixo dele.
2. Na janela **Seleccionar Local de Restauro** , pode usar quer o local original, sem quaisquer alterações, ou especificar outro local para o qual restaurar o ficheiro.

   Clique em **Explorar** para escolher onde guardar a sua tarefa de backup.

Nota
Não se esqueça de clicar em **Restaurar** para iniciar ou **Cancelar** para parar. Para refinar as suas definições, clique em **Opções**.

Caixa de Diálogo Opções de Restaurar

As opções de restaurar permitem especificar se os ficheiros a serem restaurados já existem no destino na altura do restauro em si, e se actualiza a data modificada de cada ficheiro restaurado.

Quando os ficheiros a restaurar já existem

- **Substituir Antigos** O BitDefender substitui apenas os ficheiros antigos. Os ficheiros antigos são determinados baseado na data em que foram modificados.

Data de Modificação do Ficheiro

Se a opção for seleccionada, o BitDefender usa a data actual para indicar a data em que os ficheiros ou directórios foram restaurados. Se não, o BitDefender usa a data de modificação do ficheiro ou directório de quando foi feito o backup.

Estrutura de Directório

Só se torna activa quando escolhe outro local para onde restaurar os dados. Pode também preservar a estrutura de directório dos seus dados.

Controlo de Tarefas

Existem três formas de monitorizar uma tarefa: pausar a tarefa, parar a tarefa e parar todas.

Pausa

Para por em pausa um backup que está a decorrer ou uma tarefa de restauro, clique no botão **Pausar Tarefa** no menu **Controlo de Tarefa** .

Parar

Para parar um backup que está a decorrer ou uma tarefa de restauro, clique no botão **Parar Tarefa** no menu **Controlo de Tarefa** .

Parar Tudo

Se existe mais do que uma tarefa de backup ou restauro a decorrer, não há necessidade de as parar uma a uma. Clique no botão **Parar Todas** no menu **Controlo de Tarefa** para as parar todas de uma só vez.

23.3.3. Visualizador de Relatórios

Esta secção mostra-lhe como ver, importar, exportar e limpar logs. A opção de Logs ajuda-o a lembrar do que fez backup ou restaurou e quando o fez e também mostra os avisos de erro das operações. Por exemplo, se um erro ocorreu quando um ficheiro foi lido durante a execução, o BitDefender regista-a como uma mensagem de aviso.

Pode mudar para **Visualizar Log** ao fazer uma das coisas seguintes:

- Clique em **Visualizar Log** na **Barra de Navegação**.
- Clique em **Ver** na **Barra de Menu** e seleccione **Visualizar Log**.
- Use um atalho ao premir as seguintes teclas **CTRL+Alt+L**.

Histórico

A opção de visualização de relatórios permite rastrear a sua operação, e descobrir a razão para a mesma ter falhado.

A descripção de um item de um log do Backup BitDefender contém os seguintes elementos:

Tipo

Uma classificação da severidade do item no log. Existem quatro graus de severidade no Backup BitDefender:

- **Fatal:** Um problema significativo que previne que o Backup BitDefender de decorrer normalmente. Por exemplo, o ficheiro de configuração do Backup BitDefender foi danificado.
- **Erro:** Um problema que leva a uma falha da operação. Por exemplo, uma tarefa que é backup num servidor, mas o servidor não pode ser acedido.
- **Aviso:** um problema que não afecta uma operação, mas que pode mais tarde ser classificado como um evento. Por exemplo, um ficheiro que não pode ser lido durante o backup.
- **Informação:** Descreve uma operação bem-sucedida. Por exemplo, uma tarefa foi apagada com sucesso.

Data

A data em que o item do log ocorreu.

Tempo

A hora local em que o item do log ocorreu.

Origem

A fonte que fez o log do respectivo item, que pode ser uma tarefa ou a aplicação do Backup BitDefender. Por exemplo, um item de sistema marcado indica que foi posto no log pela aplicação do Backup BitDefender. Outras possíveis marcas são os nomes das tarefas do Backup BitDefender terem feito log do respectivo item.

Utilizador
O nome do utilizador conforme com a acção do item que foi log.

Descrição
Apresenta o conteúdo detalhado do item que foi log.

Limpar

O Backup BitDefender fornece duas formas de limpar logs: automaticamente e manualmente.

Importante

Uma vez que o registo de log tenha sido limpo, não pode mais ser recuperado. Logo é melhor exportar os logs para um ficheiro e preservá-los para futura consulta.

Limpar Automaticamente
Quando o Backup BitDefender inicia, compara o tamanho do log existente com o tamanho do log por defeito. O Backup BitDefender limpa automaticamente todos os ficheiros de log que excedam o tamanho por defeito.

Nota

Para saber mais ou modificar o tamanho por defeito do log siga os seguintes passos:

1. Clique em **Ferramenta** na **Barra de Menu**.
2. Clique em **Opções**, e depois seleccione **Relatórios & Log**.
3. Insira a desejada limitação de tamanho (em MB) no campo correspondente. Quando o ficheiro de log o atingir como limite, o Backup BitDefender limpará todos os logs.

Limpar Manualmente
Siga estes passos para limpar logs manualmente.

1. Clique em **Limpar Todos** no menu **Gestão de Logs** .
2. Clique em **OK** para exportar certos registos antes de limpar os outros, ou clique **Não** se não desejar preservar quaisquer registos.

Importar e Exportar Logs

O Backup BitDefender suporta actualmente importação e exportação de ficheiros em dois formatos: `.TXT` e `.XML`

Nota

Recomendamos que exporte e guarde o log para um ficheiro antes de o limpar.

Para exportar os logs para um ficheiro especificado, siga estes passos:

1. Clique em **Exportar para ficheiro .TXT** ou **Exportar para ficheiro .XML** no menu **Gestão de Logs** .

2. Insira o nome do ficheiro e seleccione o local para onde guardar o ficheiro.
3. Clique em **Guardar**.

Para importar logs de um ficheiro específico, siga estes passos:

1. Clique em **Importar para ficheiro .TXT** ou **Importar para ficheiro .XML** no menu **Gestão de Logs** .
2. Encontrar o seu ficheiro.
3. Clique em **Abrir**.

Nota

Clique no botão **Actualizar** no menu **Gestão de Logs** para ter a certeza que vê os logs mais recentes.

23.3.4. Caixa de Ferramentas

Esta secção mostra como usar o Backup BitDefender para gravar dados num CD/DVD ou para gravar um ficheiro de imagem ISO. Abrange assuntos tais como gravar um CD-R/RW, DVD-R/RW/RAM, DVD+R/RW/DL e preservar dados em backup offline.

Pode mudar para **Toolbox** fazendo uma das coisas seguintes:

- Clique em **Toolbox** na **Barra de Navegação**.
- Clique em **Ver** na **Barra de Menu** e seleccione **Toolbox**.
- Use um atalho premindo as teclas **CTRL+Alt+T**.

Gravar para CD/DVD

Para gravar manualmente num CD/DVD, siga estes passos:

1. Clique em **Gravar dados no CD/DVD**.
2. Clique em **Apagar** se deseja reutilizar um disco regravável. Se deseja apagar o seu conteúdo rapidamente, clique em **Rápido**. Se necessita de apagar a informação de gravação completamente, clique em **Completa**, mas esta levará algum tempo.
3. Clique em **Gravar com Diálogo**.

   Aqui é onde pode definir que o disco seja ejectado após a gravação ter terminado (se deseja partilha-lo com outros) ou escrito usando o ficheiro de sistema Joliet (menos restrições no nome do ficheiro).
4. Clique em **Ficheiro** ou **Directório** nos pop-ups da caixa de diálogo para adicionar dados que deseja gravar.
5. Após os dados terem sido adicionados, seleccione o gravador e insira o nome do disco onde vai gravar os dados, e depois clique em **Gravar**.

Gravar um ficheiro de imagem ISO para um CD/DVD

Para gravar um ficheiro de imagem ISO para um CD/DVD siga estes passos:

1. Clique em **Gravar um ficheiro de imagem ISO para um CD/DVD**.

2. Clique em **Apagar** se deseja reutilizar um disco regravável. Se deseja apagar o seu conteúdo rapidamente, clique em **Rápido**. Se necessita de apagar a informação de gravação completamente, clique em **Completa**, mas esta levará algum tempo.
3. Clique em **Gravar com Diálogo**.

   É aqui que pode definir ejectar o seu disco após gravação, finalizar o disco (se desja partilhá-lo com outros) ou escrever os dados usando o ficheiro de sistema Joliet (menos restrições de nome do ficheiro).
4. Prima **Adicionar**.
5. Seleccione um ficheiro de imagem ISO para gravar e clique em **Abrir**.
6. Clique em **Gravar**.

Gerir o Meu Gravador

Isto ajuda-o a gerir e ver o dispositivo de gravação e de media do sistema actual. Contém os seguintes links:

- **Ejectar Dispositivo** Ejecta o dispositivo de gravação seleccionado.
- **Fechar Dispositivo** Fecha o dispositivo de gravação seleccionado.
- **Infos de Media** Permite visualizar a informação de Media do dispositivo de gravação.
- **Infos de Dispositivo** Permite visualizar a informação do dispositivo de gravação.
- **Capacidades** Permite visualizar as capacidades de gravação de media.
- **Apagar Media** Apaga o conteúdo do disco.

23.3.5. Barra de Menu

Existem seis menus que pode usar para executar todas as funções oferecidas pela solução de backup BitDefender.

Ficheiro

- **Criar Nova tarefa:** Mostra uma caixa de diálogo de forma a criar uma nova tarefa de backup ou outra tarefa.
- **Abrir o Backup Set:** - Mostra uma caixa de diálogo de forma a abrir o backup set ou o catalog set para restauro.
- **Sair:** Permite sair da secção de backup BitDefender.

Tarefa

- **Backup:** Executa o backup de uma tarefa seleccionada. Se existe mais do que uma tarefa seleccionada, executa todas as tarefas seleccionadas.
- **Restaurar Ficheiro:** Restaura a tarefa seleccionada. Se existe mais do que uma tarefa seleccionada, executa todas as tarefas seleccionadas .
- **Restaurar Dados em Ponto-Tempo:** Restaura a tarefa seleccionada para um determinado ponto do tempo. Se existe mais do que uma tarefa seleccionada, executa todas as tarefas seleccionadas.
- **Agendar:** Cria a tarefa agendada ou modifica a que já existe.

- **Apagar Agendar:** - Elimina o agendamento da tarefa agendada.
- **Apagar:** - elimina a tarefa seleccionada. Se existe mais do que uma tarefa seleccionada, executa todas as tarefas seleccionadas.
- **Apagar Todas** - Elimina todas as tarefas no gestor de tarefas.
- **Explorar Destino:** Permite ver os dados do backup do destino da tarefa seleccionada.
- **Modificar Opções:** Modifica opções das tarefas seleccionadas.
- **Propriedades:** - PErmite modificar as propriedades de uma tarefa seleccionada, incluindo a fonte dos dados, nome, destino, etc, da tarefa.

Relatório

- **Ver Relatório:** Se a tarefa seleccionada contém definições de segurança, esta opção permite ver os conteúdos do relatório da tarefa.
- **Guardar como:** Guarda o conteúdo do relatório seleccionado para um determinado ficheiro.
- **Imprimir:** Imprime o conteúdo do relatório seleccionado.
- **Apagar Tudo:** - Apaga o conteúdo do relatório da tarefa seleccionada.
- **Actualizar:** Actualiza o conteúdo do relatório da tarefa seleccionada.

Ver

- **Introdução:** Se a janela da introdução não estiver a ser mostrada, esta opção permite abri-la.
- **Gestor de Tarefa:** Se a janela do gestor de tarefa não estiver a ser mostrada, esta opção permite abri-la.
- **Ver Log:** Se a janela do visualizador de logs não estiver a ser mostrada, esta opção permite abri-la.
- **Toolbox:** Se a janela não estiver a ser mostrada, esta opção permite abri-la.
- **Mostrar Barra de Menu:** Esconde a Barra de Menu. Para a mostrar, apenas prima **ALT**.
- **Mostrar Linha de Grelha:** Mostra ou esconde a linha de grelha. Aplica-se ao visualizador de logs e ao gestor de tarefas windows.

Ferramenta

- **Assistente de Backup:** Inicia o assistente de backup.
- **Assistente de Restauro** - Inicia o assistente de restauro.
- **Gravar:** Inicia a ferramenta de gravação de CD/DVD/ISO ou a ferramenta de gestão da gravação.
  - **Gravar CD/DVD**
  - **Gravar Ficheiros ISO**
  - **Ver Info Gravador**
- **Exportar todas Tarefas:** Exporta todas as tarefas criadas para um ficheiro específico.
- **Importar Tarefas:** Importa tarefas de um ficheiro `.JOB`, um ficheiro `.TXT` , ou um ficheiro `.XML`.
- **Exportar Logs:** Exporta relatórios para um ficheiro `.TXT` ou um ficheiro `.XML` .

- Para um ficheiro TXT
- Para um ficheiro XML
- **Importar Logs:** Importa logs de um ficheiro .TXT ou de um ficheiro .XML .
  - De um ficheiro TXT
  - De um ficheiro XML
- **Opções:** Modifica as suas opções gerais de backup.
  - **Geral**
  - **Relatórios & Registos**
  - **Agendar Tarefa**

Ajuda

- **Tópico de Ajuda:** Mostra tópicos de ajuda.
- **Procurar:** Permite procurar tópicos de ajuda baseado nas palavras chave inseridas ou seleccionadas.
- **BitDefender no Website:** Permite aceder à página da Internet do BitDefender e aceder às notícias BitDefender e ao suporte online.
- **Informação de Suporte:** Fornece informações sobre como entrar em contato com a BitDefender para ajudar e suporte.
- **Acerca do Backup BitDefender :** Mostra o copyright, versão, e edição da info relacionada com o Backup BitDefender .

24. Encriptação de Chat

O conteúdo das suas mensagens instantâneas deve permanecer entre si e a pessoa com quem conversa.Ao encriptar as suas conversas, tem a garantia que, se alguém tentar interceptá-las não conseguirá ler o conteúdo.

Por defeito, o BitDefender encripta todas as suas sessões de mensagens instantâneas desde que:

- O seu companheiro de conversação possui a versão BitDefender instalada que suporta a Encriptação de Conversas e esta está activada para a aplicação de conversação utilizada.
- Você ou o seu companheiro de conversação utilizam o Yahoo Messenger ou o Windows Live (MSN) Messenger.

Importante

BitDefender não irá encriptar uma conversação se o parceiro usar uma aplicação de chat web-based, tal como a Meebo, ou se um parceiro de conversação usar o Yahoo Messenger e o outro usar o Windows Leve (MSN).

Para configurar a encriptação de mensagens instantâneas:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Encriptação > Encriptação de Conversas**.

Nota

Pode configurar facilmente a encriptação de mensagens instantâneas para cada parceiro com a barra de ferramentas do BitDefender na janela de conversação.

Por defeito, a Encriptação de Mensagens Instantâneas está activada para o Yahoo Messenger e o Windows Live (MSN) Messenger.Pode escolher desactivar a encriptação de Mensagens Instantâneas para apenas uma aplicação de chat ou para todas.

São mostradas duas tabelas:

- **Exclusões da Encriptação** - lista os IDs dos utilizadores e o programa de IM associado para os quais a encriptação está desactivada.Para remover um contacto da lista , seleccione-o e clique no botão **Remover**.
- **Ligações Actuais** - lista as actuais ligações de mensagens (IDs dos utilizadores e o programa de IM associado) e se devem ou não ser encriptadas.Uma ligação poderá não ser encriptada pelas seguintes razões:
  - Desactivou explicitamente a encriptação para o respectivo contacto.

- O seu contacto não tem instalado uma versão do BitDefender que suporte a encriptação IM.

24.1. Desactivar a Encriptação para Utilizadores Específicos

Para desactivar a encriptação para um determinado utilizador, siga estes passos:

1. Clique no botão **Adicionar** para abrir a janela de configuração.
2. Insira no campo de edição o ID do utilizador do seu contacto.
3. Seleccione a aplicação de mensagens instântaneas associada ao contacto.
4. Clique em **OK**.

24.2. Barra de Ferramentas do BitDefender na Janela de Conversação

Pode configurar facilmente a encriptação de conversas instantâneas com a barra de ferramentas do BitDefender na janela de conversação.

A toolbar deve de estar no canto inferior direito da janela de chat. Procure aí o logo do BitDefender.

Nota

A toolbar indica que a conversação é encriptada ao mostrar um pequena chave ao pé do logo do BitDefender.

Ao clicar na toolbar do BitDefender são-lhe apresentadas as seguintes opções:

- **Desactivar permanentemente a encriptação para o `contacto`.**
- **Convidar `contacto` a usar a encriptação.** Para encriptar as suas conversações, o seu contacto deve de instalar o BitDefender e usar um programa de MI compatível.
- **Adicionar `contacto` à lista negra do Controlo Parental.** Se adicionar um contacto à lista negra do Controlo Parental e o mesmo estiver ligado, não terá mais acesso às mensagens instântaneas enviadas por esse contacto.Para remover o contacto da lista negra, clique na barra de ferramentas e seleccione **Remover `contacto` da lista negra do Controlo Parental**.

25. Encriptação Ficheiro

O Cofre de Ficheiros BitDefender permite-lhe criar drives lógicas encriptadas, e protegidas por palavra-passe (cofres) no seu computador onde pode armazenar em segurança os seus documentos confidenciais e sensíveis.Os dados armazenados nos cofres apenas podem ser acedidos pelos utilizadores que sabem a palavra-passe.

A palavra-passe permite-lhe abrir, armazenar dados no cofre e fechá-lo ao mesmo tempo que o mantém seguro.Quando um cofre é aberto, pode adicionar-lhe ficheiros, aceder aos que lá estão ou alterá-los.

Fisicamente, o cofre é um ficheiros armazenado no seu disco duro local com a extensão `.bvd`.Apesar dos ficheiros físicos que representam as drives de cofre poderem ser acedidos a partir de um sistema operativi diferente (tal como Linux), a informação armazenada não pode ser lida por estar encriptada.

A Encriptação de Ficheiros está activada por defeito.Para desactivar, siga os seguintes passos:

1. Clique com o botão direito do rato no ícone do BitDefender no tabuleiro de sistema e seleccione **Preferências**.
2. Na janela de Preferências que aparece, clique no botão que corresponde à **Encriptação de Ficheiros**.

Se desactivar o Cofre de Ficheiros, todos os cofres de ficheiros serão fechados e não será mais capaz de aceder aos ficheiros que eles contêm.

Os sofres de ficheiros podem ser geridos a partir da janela do BitDefender ou com o menu contextual do Windows e da unidade lógica associada ao cofre.

25.1. Gerir Cofres de Ficheiros no Interface do BitDefender

A forma como pode aceder e gerir os seus cofres de ficheiros difere consoante o modo de interface que utiliza. A seguinte secção explica como pode gerir cofres de ficheiros.

25.1.1. Criar Cofre

Para criar um novo cofre, vá a **Encriptação > Encriptação de Ficheiros** no Modo Avançado e faça uma das seguintes acções:

- Clique **Criar cofre**.
- Clique botão direito do rato na tabela dos cofres e seleccionar **Criar**.

Para criar um novo cofre, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio

Em **Armazenamento de Ficheiros** clique em **Criar Cofre de Ficheiros** na área de Encriptação de Ficheiros.

Modo Avançado

Vá a **Encriptação > Encriptação de Ficheiros** no Modo Avançado e faça uma das seguintes acções:

- Clique **Criar cofre**.
- Clique botão direito do rato na tabela dos cofres e seleccionar **Criar**.

Uma nova janela irá aparecer.Proceder da seguinte forma:

1. Especificar a localização e o nome do cofre de ficheiros.
   - Clique em **Explorar** para seleccionar a localização do cofre e guarde o cofre de ficheiros sob o nome desejado.
   - Escreva nos respectivos campos o nome e o caminho do cofre de ficheiros no disco.
2. Escolha a letra da drive a partir do menu.Quando abre o cofre, um disco virtual com a letra seleccionada aparecerá em O Meu Computador.
3. Se deseja mudar o tamanho por defeito (50 MB) do cofre, insira o valor desejado no campo **Tamanho Cofre** .
4. Escreva a palavra-passe desejada para o cofre na**Palavra-passe**e**Confirmar**campos.Qualquer pessoa que tente abrir o cofre e aceder aos seus ficheiros tem de inserir a palavra-passe.
5. Clique em **Criar** se deseja criar o cofre na localização seleccionada.Para criar e mostrar o cofre como um disco virtual em O Meu Computador, clique em **Criar&Abrir**.

O BitDefender informá-lo-á imediatamente do resultado da operação.Se ocorreu um erro, use a mensagem de erro para resolver o mesmo.Clique **OK** para fechar a janela.

Nota

Poderá ser conveniente que guarde todos os cofres de ficheiros no mesmo local. Desta forma poderá localizá-los mais rapidamente.

25.1.2. Abrir Cofre

De forma a poder aceder e trabalhar com os ficheiros armazenados no cofre, tem de o abrir.Quando abre o cofre, um disco virtual aparece em O Meu Computador.A drive tem a denominação da letra que atribuiu ao cofre.

Para abrir um cofre, siga estes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Encriptação > Encriptação de Ficheiros** e faça uma das seguintes acções:
   - Seleccione o cofre da tabela e clique **Abrir cofre**.
   - Clique com o botão-direito na tabela e seleccione **Abrir**.

   Nota
   Se um cofre anteriormente criado não aparecer na tabela, clique em **Procurar cofre** e vá primeiro para a respectiva localização.

   Uma nova janela irá aparecer.
3. Escolha a letra da drive a partir do menu.
4. Insira a palavra-passe do cofre no campo **Palavra-passe** .
5. Clique em **Abrir**.

O BitDefender informá-lo-á imediatamente do resultado da operação.Se ocorreu um erro, use a mensagem de erro para resolver o mesmo.Clique **OK** para fechar a janela.

25.1.3. Fechar Cofre

Quando terminou de trabalhar sobre um cofre de ficheiros, deve de o fechar de forma a proteger os seus dados.Ao fechar o cofre, o correspondente disco virtual desaparecerá de O Meu Computador. Logo, o acesso aos dados armazenados no cofre fica completamente bloqueado.

Para fechar um cofre, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
Vá a **Armazenamento de Ficheiros** e efectue uma das seguintes acções:

- Clique em **Fechar Cofre de Ficheiros** na área das Tarefas Rápidas.
- Clique no cofre de ficheiros na área de **Encriptação de Ficheiros** e seleccione **Fechar** no menu que aparece.

Aparecerá um assistente que ajudará a fechar o cofre.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Eleger Cofre**

   Aqui é onde pode especificar o cofre a fechar.
2. **Confirmar**

   Aqui é onde pode rever as operações escolhidas.

3. **Terminar**

   Aqui é onde poder ver o resultado da operação.

Modo Avançado

Vá a **Encriptação > Encriptação de Ficheiros** e faça uma das seguintes acções:

- Seleccione o cofre na tabela e clique em **Fechar cofre**.
- Clique com o botão-direito do rato no cofre da tabela e seleccione **Fechar**.

O BitDefender informá-lo-á imediatamente do resultado da operação.Se ocorreu um erro, use a mensagem de erro para resolver o mesmo.Clique **OK** para fechar a janela.

25.1.4. Alterar Palavra-passe do Cofre

O cofre tem de ser fechado antes que possa mudar a sua palavra-passe.Para alterar a palavra-passe de um cofre, vá a **Encriptação > Encriptação de Ficheiros** no Modo Avançado e faça uma das seguintes acções:

- Seleccione o cofre na tabela e clique em **Alterar palavra-passe**.
- Clique com o botão-direito do rato no cofre da tabela e seleccione **Alterar palavra-passe**.

Uma nova janela irá aparecer.Proceder da seguinte forma:

1. Insira a palavra-passe actual do cofre no campo **Palavra-passe antiga** .
2. Insira a nova palavra-passe nos campos **Nova palavra-passe** e **Confirmar nova palavra-passe** .

Nota

A palavra-passe tem de ter pelo menos 8 caracteres.Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

3. Clique em **OK** para alterar a palavra-passe.

O BitDefender informá-lo-á imediatamente do resultado da operação.Se ocorreu um erro, use a mensagem de erro para resolver o mesmo.Clique **OK** para fechar a janela.

25.1.5. Adicionar Ficheiros ao Cofre

Para adicionar ficheiros a um cofre, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio

Em **Armazenamento de Ficheiros** clique em **Adicionar Ficheiro ao Cofre** na área de Tarefas Rápidas.

Aparecerá um assistente que ajudará a adicionar ficheiros ao cofre.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Seleccionar ficheiros & pastas**

   Clique em **Adicionar alvo** para seleccionar os ficheiros/pastas que serão adicionados ao cofre.

2. **Eleger Cofre**

   Pode seleccionar um cofre existente, procurar um cofre anteriormente criado ou criar um novo cofre ao qual pretende adicionar os ficheiros.

3. **Criar Cofre**

   Ao criar um novo cofre, tem de especificar aqui as informações necessárias. Para saber mais, por favor consulte“*Criar Cofre*” (p. 174)

4. **Inserir palavra-passe**

   Se seleccionou um cofre fechado, tem de introduzir a palavra-passe para o abrir.

5. **Confirmar**

   Aqui é onde pode rever as operações escolhidas.

6. **Conteúdo do Cofre**

   Aqui é onde pode ver o conteudo do cofre.

Modo Avançado

1. Vá a **Encriptação > Encriptação de Ficheiros**.
2. Seleccione da tabela de cofres o cofre para onde quer adicionar ficheiros.
3. Se o cofre estiver fechado, deve em primeiro lugar abri-lo (clicar botão direiro do rato sobre ele e seleccionar **abrir cofre**).
4. Clique **Adicionar ficheiro**.Uma nova janela irá aparecer.
5. Seleccione os ficheiros / pastas que deseja adicionar ao cofre.
6. Clique em **OK** para copiar os objectos seleccionados para o cofre.

25.1.6. Remover os ficheiros do Cofre

Para remover um ficheiro de um cofre, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio

Em **Armazenamento de Ficheiros** clique em **Remover Ficheiros de Cofre** na área de Tarefas Rápidas.

Aparecerá um assistente que ajudará a remover ficheiros do cofre.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Eleger Cofre**

   Aqui é onde pode seleccionar o cofre de onde deseja remover ficheiros.

2. **Inserir palavra-passe**

   Se seleccionou um cofre fechado, tem de introduzir a palavra-passe para o abrir.

3. **Conteúdo do Cofre**

   Seleccione os ficheiros/pastas ser serão removidos do cofre.

4. **Confirmar**

   Aqui é onde pode rever as operações escolhidas.

5. **Terminar**

   Aqui pode ver o resultado da operação.

Modo Avançado

Vá a **Encriptação > Encriptação de Ficheiros** e siga os seguintes passos:

1. Seleccione da tabela de cofres o cofre que contém o ficheiro a ser removido.
2. Se o cofre estiver fechado, deve em primeiro lugar abri-lo (clicar botão direiro do rato sobre ele e seleccionar **abrir cofre**).
3. Seleccione o ficheiro a ser removido a partir da tabela que mostra o conteúdo do cofre.
4. Clique **Remover ficheiros/pastas**.

25.1.7. Ver Conteúdo do Cofre

Para ver o conteúdo de um cofre de ficheiros, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio

Vá a **Armazenamento de Ficheiros** e efectue uma das seguintes acções:

- Clique em **Ver Cofre de Ficheiros** na área das Tarefas Rápidas.
- Clique no cofre de ficheiros na área de **Encriptação de Ficheiros** e seleccione **Ver** no menu que aparece.

Aparecerá um assistente que ajudará a ver os ficheiros do cofre.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Eleger Cofre**

   Aqui é onde pode seleccionar o cofre de onde deseja ver os ficheiros.

2. **Inserir palavra-passe**

   Se seleccionou um cofre fechado, tem de introduzir a palavra-passe para o abrir.

3. **Confirmar**

   Aqui é onde pode rever as operações escolhidas.

4. **Conteúdo do Cofre**

   Aqui pode ver o resultado da operação.

Modo Avançado

Vá a **Encriptação > Encriptação de Ficheiros** e siga os seguintes passos:

1. Seleccione na tabela de cofres aquele cujo conteúdo pretende visualizar.
2. Se o cofre estiver fechado, deve em primeiro lugar abri-lo (clicar botão direiro do rato sobre ele e seleccionar **abrir cofre**).
3. A tabela do fundo mostra o conteúdo dos cofre seleccionado.

25.1.8. Eliminar Cofre de Ficheiros

Para eliminar um cofre de ficheiros, siga estes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Intermédio**.
2. Vá a **Armazenamento de Ficheiros**.
3. Clique no cofre de ficheiros na área de **Encriptação de Ficheiros**.
4. Se o cofre estiver aberto, seleccione **Fechar** no menu que aparece e clique novamente no cofre.Se o cofre estiver fechado, siga para o passo seguinte.
5. Seleccione **Eliminar** no menu que aparece.

Importante

Se eliminar um cofre de ficheiros, eliminará também o conteúdo.

25.2. Gerir Cofres de Ficheiros no Windows

O BitDefender está integrado no Windows para o ajudar a gerir mais facilmente os seus cofres de ficheiros.

O menu contextual do Windows aparece sempre que clica com o botão direito do rato sobre um ficheiro ou pasta do seu computador ou sobre um objecto do seu ambiente de trabalho.Aponte o cursor do rato para Cofre de Ficheiros BitDefender neste menu e terá acesso a todas as operações disponíveis.

Além disso, sempre que abre (instala) um cofre, aparecerá uma nova partição lógica (nova unidade).Abra O Meu Computador e verá uma nova drive baseada no cofre de ficheiros. Será capaz de fazer operações com ficheiros nele (copiar, apagar, alterar, etc.). Os ficheiros estão protegidos na medida em que estejam residentes nesta drive (porque é necessária uma palavra-passe para a operação de montagem).Quando terminar, fechar (desmontar) o seu cofre de forma a iniciar a protecção do seu conteúdo.

Pode facilmente identificar os cofres de ficheiros BitDefender no seu computador pelo icone BitDefender e pela extensão `.bvd`.

25.2.1. Criar Cofre

Mantenha em mente que um cofre é na realidade apenas um ficheiro com a extensão `.bvd`.Só quando abre o ficheiro, é que uma drive de disco virtual aparece em O Meu Computador e pode, de forma segura, armazenar ficheiros no seu interior. Quando cria um cofre, deve de especificar onde e sobre que nome o deve de guardar no seu computador. Deve também de especificar uma palavra-passe para proteger o seu conteúdo.Apenas os utilizadores que sabem a palavra-passe podem abrir o cofre e aceder aos documentos e dados armazenados no seu interior.

Para criar um cofre, siga estes passos:

1. Clique no botão direito do rato no seu Ambiente de Trabalho ou numa pasta do seu computador, aponte para **Cofre Ficheiros BitDefender** e seleccione **Criar**.Uma nova janela irá aparecer.
2. Especificar a localização e o nome do cofre de ficheiros.
   - Clique em **Explorar** para seleccionar a localização do cofre e guarde o cofre de ficheiros sob o nome desejado.
   - Escreva nos respectivos campos o nome e o caminho do cofre de ficheiros no disco.
3. Escolha a letra da drive a partir do menu.Quando abre o cofre, um disco virtual com a letra seleccionada aparecerá em O Meu Computador.
4. Escreva a palavra-passe desejada para o cofre na**Palavra-passe**e**Confirmar**campos.Qualquer pessoa que tente abrir o cofre e aceder aos seus ficheiros tem de inserir a palavra-passe.
5. Seleccione **Formatar drive** para formatar a drive virtual atribuida ao cofre.Deve de formatar primeiro a drive antes de adicionar ficheiros ao cofre.

6. Se deseja mudar o tamanho por defeito (50 MB) do cofre, insira o valor desejado no campo **Tamanho Cofre** .
7. Clique em **Criar** se deseja criar o cofre na localização seleccionada.Para criar e mostrar o cofre como um disco virtual em O Meu Computador, clique em **Criar&Abrir**.

O BitDefender informá-lo-á imediatamente do resultado da operação.Se ocorreu um erro, use a mensagem de erro para resolver o mesmo.Clique **OK** para fechar a janela.

Nota
Poderá ser conveniente que guarde todos os cofres de ficheiros no mesmo local. Desta forma poderá localizá-los mais rapidamente.

25.2.2. Abrir Cofre

De forma a poder aceder e trabalhar com os ficheiros armazenados no cofre, tem de o abrir.Quando abre o cofre, um disco virtual aparece em O Meu Computador.A drive tem a denominação da letra que atribuiu ao cofre.

Para abrir um cofre, siga estes passos:

1. Localize no seu computador o ficheiro `.bvd` que representa o cofre que deseja abrir.
2. Clique com o botão-direito no ficheiro, aponte para **Cofre Ficheiros BitDefender** e seleccione **Abrir**.Uma alternativa mais rápida seria fazer duplo clique sobre o ficheiro, ou clicar com o botão-direito do rato sobre ele e seleccionar **Abrir**.Uma nova janela irá aparecer.
3. Escolha a letra da drive a partir do menu.
4. Insira a palavra-passe do cofre no campo **Palavra-passe** .
5. Clique em **Abrir**.

O BitDefender informá-lo-á imediatamente do resultado da operação.Se ocorreu um erro, use a mensagem de erro para resolver o mesmo.Clique **OK** para fechar a janela.

25.2.3. Fechar Cofre

Quando terminou de trabalhar sobre um cofre de ficheiros, deve de o fechar de forma a proteger os seus dados.Ao fechar o cofre, o correspondente disco virtual desaparecerá de O Meu Computador. Logo, o acesso aos dados armazenados no cofre fica completamente bloqueado.

Para fechar um cofre, siga estes passos:

1. Abra O Meu Computador (clique em start menu Inciar do Windows, e depois **O Meu Computador**.

2. Identifique a drive de disco virtual correspondente ao cofre que deseja fechar.Procure a letra da drive virtual que atribuiu ao cofre quando o abriu.
3. Clique com o botão-direito do rato no correspondente disco virtual em O Meu Computador, aponte para **Cofre Ficheiros BitDefender** e seleccione **Fechar**.

Também pode clicar com o botão direito do rato .bvd no ficheiro que representa o cofre, apontar para **Cofre de Ficheiros BitDefender** e clicar em **Fechar**.

O BitDefender informá-lo-á imediatamente do resultado da operação.Se ocorreu um erro, use a mensagem de erro para resolver o mesmo.Clique **OK** para fechar a janela.

Nota

Se diversos cofres estiverem abertos, deve usar o interface do BitDefender em Modo Avançado.Se for à barra **Encriptação**, Cofre de Ficheiro, poderá visualizar uma tabela que lhe dá informação sobre os cofres existentes. Esta informação inclui sobre se o cofre está aberto e, se sim, qual a letra da drive que lhe está atribuida.

25.2.4. Adicionar ao Cofre de Ficheiros

Antes que possa adicionar ficheiros ou pastas ao cofre, deve de abri-lo.Uma vez que um cofre esteja aberto, pode facilmente armazenar ficheiros ou pastas no seu interior usando o menu contextual.Clique com o botão-direito no ficheiro ou pasta que deseja copiar para o cofre, aponte para **Cofre Ficheiros BitDefender** e seleccione **Adicionar ao Cofre de Ficheiros**.

- Se apenas um cofre estiver aberto, o ficheiro ou pasta é copiado directamente para esse cofre.
- Se vários cofres estiverem abertos, ser-lhe-á solicitado que escolha o cofre para onde deseja copiar o item. Seleccione do menu a letra da drive correspondente ao cofre desejado e clique **OK** para o copiar.

Pode sempre usar a drive virtual correspondente ao cofre.Siga estes passos:

1. Abra O Meu Computador (clique em start menu Inciar do Windows, e depois **O Meu Computador**.
2. Insira a drive virtual correspondente ao cofre.Procure a letra da drive virtual que atribuiu ao cofre quando o abriu.
3. Copiar-colar ou drag&drop os ficheiros ou pastas directamente para a drive virtual.

25.2.5. Remover do Cofre de Ficheiros

De forma a remover os ficheiros ou pastas do cofre, o cofre deve de ser aberto.Para remover os ficheiros ou pastas do cofre, siga os seguintes passos:

1. Abra O Meu Computador (clique em start menu Inciar do Windows, e depois **O Meu Computador**.

2. Insira a drive virtual correspondente ao cofre.Procure a letra da drive virtual que atribuiu ao cofre quando o abriu.
3. Remover os ficheiros ou pastas como normalmente faz no Windows (por exemplo, clique botão-direito no ficheiro que quer apagar e seleccione **Apagar**).

25.2.6. Alterar Palavra-passe do Cofre

A palavra-passe protege o conteúdo do cofre contra acessos não-autorizados.Apenas os utilizadores que sabem a palavra-passe podem abrir o cofre e aceder aos documentos e dados armazenados no seu interior.

O cofre tem de ser fechado antes que possa mudar a sua palavra-passe.Para mudar a palavra-passe do cofre, siga os seguintes passos:

1. Localize no seu computador o ficheiro `.bvd` que representa o cofre.
2. Clique com o botão-direito do rato no ficheiro, aponte para **Cofre Ficheiros BitDefender** e seleccione **Alterar palavra-passe do cofre**.Uma nova janela irá aparecer.
3. Insira a palavra-passe actual do cofre no campo **Palavra-passe antiga** .
4. Insira a nova palavra-passe nos campos **Nova palavra-passe** e **Confirmar nova palavra-passe** .

Nota

A palavra-passe tem de ter pelo menos 8 caracteres.Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

5. Clique em **OK** para alterar a palavra-passe.

O BitDefender informá-lo-á imediatamente do resultado da operação.Se ocorreu um erro, use a mensagem de erro para resolver o mesmo.Clique **OK** para fechar a janela.

26. TUNE-UP

BitDefender vem com um módulo de Optimização que o ajuda a manter a integridade do seu sistema. As ferramentas de manutenção oferecidas são criticas para o melhoramento do desempenho do seu sistema e para uma gestão eficiente do espaço do seu disco duro.

O BitDefender fornece as seguintes ferramentas de optimização do PC:

- Desfragmentador reorganiza os dados no disco rígido de forma a que as partes constituintes de cada ficheiro sejam armazenadas juntas e de forma contínua.
- Limpeza do PC remove os ficheiros temporários da Internet e as cookies, os ficheiros não utilizados do sistema e os atalhos recentes dos documentos.
- O Localizador de Duplicados encontra e apaga ficheiros que se encontram duplicados no seu sistema.
- Limpar Registo identifica e apaga referências orfãs ou inválidas do Registo do Windows.De forma a manter o Registo do Windows limpo e optimizado, é recomendável que execute o seu Limpa Registo uma vez por mês.
- O Restaurar Registo pode recuperar as chaves de registo previamente apagadas do Registo do Windows no uso do Limpa Registo BitDefender.
- Destruidor Ficheiros apaga permanentemente os ficheiros e os seus vestígios do sistema.
- Monitor de Desempenho monitoriza a configuração do hardware e software do seu sistema de modo a garantir que está totalmente protegido contra malware.

26.1. Desfragmentar Volumes de Discos Duros

Quando copia um ficheiro que excede o tamanho do maior bloco de espaço livre no disco duro, a fragmentação do ficheiro ocorre. Porque não existe suficiente espaço livre para guardar o ficheiro de forma contínua, o mesmo é armazenado em diversos blocos. Quando o ficheiro fragmentado é acedido, os seus dados têm de ser lidos de diversos locais diferentes.

É recomendável que desfragmente o seu disco duro de forma a que:

- aceda mais rápido aos ficheiros.
- melhore o desempenho do sistema em geral.
- aumente o tempo de duração do seu disco duro.

O Assistente de Desfragmentação do Disco irá ajudar a desfragmentar o seu disco rígido.Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio

Abra o separador **Optimizar** e clique em **Desfragmentador do Disco**, na área de Tarefas Rápidas, no lado esquerdo da janela.

Modo Avançado

Vá a **Optimizar** e clique em **Executar Agora** correspondente ao Desfragmentador de PC.

Siga o procedimento de cinco passos para efectuar a desfragmentação.

1. **Escolha os discos a analisar**

   Seleccione as partições que pretende analisar para fragmentação.

2. **A analisar as partições seleccionadas**

   Aguarde que o BitDefender termine a análise das partições.

3. **Seleccione o disco a desfragmentar**

   É apresentado o estado de fragmentação das partições analisadas.Seleccione as partições que pretende desfragmentar.

4. **A desfragmentar**

   Aguarde que o BitDefender termine a desfragmentação das partições.

5. **Mostrar Resultados**

Nota

A desfragmentação poderá demorar algum tempo uma vez que involve o mover de porções de dados armazenados de um lugar para o outro do disco duro. Recomendamos que execute a desfragmentação quando não está a usar o seu computador.

26.2. Limpar o Seu PC

Cada vez que visita uma página web, são criados ficheiros temporários da Internet de forma a permitir que lhe aceda mais rapidamente da próxima vez.

Os cookies também são armazenados na seu computador quando visita uma página web.

O Assistente de Limpeza do PC ajuda-o a libertar espaço em disco e a proteger a sua privacidade ao apagar ficheiros que já não são úteis.

- Ficheiros temporários da internet e cookies do Internet Explorer.
- Ficheiros temporários da internet e cookies do Mozilla Firefox.
- ficheiros temporários do sistema que o Windows cria durante esta operação.
- recentes atalhos de documentos que o Windows cria quando abre um ficheiro.

Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Optimizar** e clique em **Limpa PC**, na área de Tarefas Rápidas, no lado esquerdo da janela.

Modo Avançado
: Vá a **Optimizar** e clique em **Executar Agora** correspondente ao Limpa PC.

Nota

Também pode adicionar um atalho a Meus Instrumentos.

Siga o procedimento de três passos para efectuar a limpeza.Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.

1. **Definir**

   Seleccione uma limpeza típica (limpar tudo) ou uma limpeza personalizada (escolher o que quer limpar).

2. **Efectuar Limpeza**

   Aguarde que o BitDefender termine a limpeza.

3. **Resultados**

26.3. Apagar Ficheiros Permanentemente

Quando apaga um ficheiro, o mesmo já não fica acessível por meios normais. No entanto o ficheiro continua armazenado no disco duro até que seja sobrescrito quando copiar para lá novos ficheiros.

O Assistente do Destruidor de Ficheiros vai ajudar a eliminar permanentemente dados removendo-os fisicamente do seu disco rígido.Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Optimizar** e clique em **Destruidor de Ficheiros**, na área de Tarefas Rápidas, no lado esquerdo da janela.

Modo Avançado
: Vá a **Optimizar** e clique em **Executar Agora** correspondente ao Destruidor de Ficheiros.

Siga o procedimento de três passos para efectuar a limpeza.Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.

1. **Seleccionar ficheiro/pasta**

   Adicione os ficheiros ou as pastas que pretende remover permanentemente.

Atenção
Não poderá recuperar ficheiros que tenham passado pelo Destruidor de Ficheiros.

2. **Destruir ficheiros**

   Aguarde que o BitDefender termine a destruição dos ficheiros.

3. **Resultados**

26.4. Limpar o Registo do Windows

Muitas aplicações escrevem chaves no Registo do Windows durante a instalação. Quando remove tais aplicações, algumas das suas chaves de registo associadas poderão não ser apagadas e continuarem no seu Registo do Windows, tornando o seu sistema mais lento e até causando instabilidade no mesmo. O mesmo acontece quando apaga atalhos para ou determinados ficheiros das aplicações instaladas no seu sistema, como também no caso de drivers corrompidos.

O Assistente de Limpeza de Registo vai ajudar a limpar o Registo do Windows e a melhorar o desempenho do seu sistema.Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Optimizar** e clique em **Limpa Registos**, na área de Tarefas Rápidas, no lado esquerdo da janela.

Modo Avançado
: Vá a **Optimizar** e clique em **Executar Agora** correspondente à Limpeza de Registos.

Nota
Também pode adicionar um atalho a Meus Instrumentos.

Siga o procedimento de quatro passos para limpar o registo.Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.

1. **Ecrã de Boas-Vindas**

2. **Efectuar Análise**

   Aguarde que o BitDefender termine a análise de registo.

3. **Seleccionar Chaves**

   Pode ver todas as chaves de registo inválidas ou orfãs detectadas. Informação detalhada é fornecida para cada chave de registo (nome, valor, prioridade, categoria).

   As chaves de registo estão agrupadas baseado na sua localização no Registo do Windows:

Categoria	Descrição
Localização Software	Chaves de registo que contêm informação sobre o caminho para as aplicações instaladas no seu computador. As chaves inválidas têm atribuida uma baixa prioridade, o que significa que as pode apagar sem qualquer risco.
Controlos Pessoais	Chaves de registo que contêm informação acerca das extensões dos ficheiros registados no seu computador.Estas chaves de registo são normalmente usadas para manter associações de ficheiros (para assegurar que o programa correcto abre quando abre um ficheiro usando o Explorador do Windows).Por exemplo, tal chave de registo permite que o Windows abra um ficheiro `.doc` com o Microsoft Word. As chaves inválidas têm atribuida uma baixa prioridade, o que significa que as pode apagar sem qualquer risco.
DLLs partilhadas	As chaves de registo que contêm informação sobre a localização das DLLs (Dynamic Link Libraries) partilhadas.Funções de armazenagem DLLs que são usadas pelas aplicações instaladas para levar a cabo certas tarefas. Podem ser partilhadas por múltiplas aplicações para reduzir os requisitos de espaço em disco e em memória. Estas chaves de registo tornam-se inválidas quando a DLL que apontam é movida para outro local ou completamente removida (isto acontece quando desinstala um programa). As chaves inválidas têm atribuidas uma prioridade média, o que significa que apagá-las pode afectar negativamente o sistema.

Por defeito, todas as chaves estão marcadas para eliminação.Pode escolher eliminar individualmente as chaves inválidas de uma determinada categoria.

Nota

Pode recuperar em qualquer momento as chaves de registo eliminadas com a Recuperação de Registos.

4. **Resultados**

26.5. Recuperar Limpeza de Registo

Por vezes, após limparmos o registo, poderá notar que o seu sistema não funciona bem ou que algumas aplicações não funcionam bem devido à falta de chaves no registo. Isto pode ser causado devido a chaves de registo partilhadas que foram apagadas durante a limpeza do registo ou por outras chaves apagadas. Para resolver este problema deverá recuperar o registo que foi limpo.

A Assistente de Recuperação de Registos vai ajudar a recuperar o registo eliminado.Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Optimizar** e clique em **Recuperação de Registos**, na área de Tarefas Rápidas, no lado esquerdo da janela.

Modo Avançado
: Vá a **Optimizar** e clique em **Executar Agora** correspondente à Recuperação de Registos.

Siga o procedimento de dois passos para recuperar o registo eliminado.Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.

1. **Seleccione o ponto de recuperação**

   Pode ver uma lista de pontos no tempo em que o Registo do Windows foi limpo.Seleccione o ponto no tempo para restaurar o Registo do Windows.

   Atenção
   A recuperação da limpeza de registo pode sobrescrever as últimas chaves do registo que foram editadas desde a última limpeza do registo.

2. **Resultados da tarefa**

26.6. Localizar Ficheiros Duplicados

Os ficheiros duplicados comem o seu espaço em disco. Imagine ter o mesmo ficheiro `.mp3` armazenado em três diferentes locais.

O Assistente do Localizador de Duplicados ajuda a detectar e eliminar os ficheiros duplicados no seu computador.Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Optimizar** e clique em **Localizador de Duplicados**, na área de Tarefas Rápidas, no lado esquerdo da janela.

Modo Avançado
: Vá a **Optimizar** e clique em **Executar Agora** correspondente ao Localizador de Duplicados.

Nota
Também pode adicionar um atalho a Meus Instrumentos.

Siga o procedimento de quatro passos para identificar e remover os duplicados.Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.

1. **Seleccionar ficheiros de destino**

   Adicione as pastas onde procurar os ficheiros duplicados.Por defeito, ficheiros com 0 KB, ficheiros nas pastas de Programas e do Windows são ignorados pois é vivamente recomendado que não elimine os ficheiros destas pastas. Clique em **Opções** se pretende adicionar algum destes ficheiros à procura.

2. **Procurar Duplicados**

   Aguarde que o BitDefender termine a procura de duplicados.

3. **Marcar ficheiros para eliminar**

   Os ficheiros idênticos estão agrupados.Pode escolher uma acção a aplicar a todos os grupos ou a cada grupo isoladamente: manter mais recente, manter mais antigo, nenhuma acção.Também pode seleccionar acções para ficheiros específicos.

   Nota
   Se não forem encontrados ficheiros duplicados, este passo será saltado.

4. **Resultados**

26.7. Monitor de Desempenho

O Monitor de Desempenho consiste numa tabela que lista os processos e as aplicações em execução, a utilização de CPU e memória e um classificação com base nesta informação.

Para aceder ao módulo do Monitor de Desempenho, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Optimizar** e clique em **Optimizador de Desempenho**, na área de Tarefas Rápidas, no lado esquerdo da janela.

Modo Avançado
: Vá a **Optimizar > Monitorizar / Optimização**.

O módulo do Monitor de Desempenho vigia constantemente a capacidade do sistema, permitindo-lhe ver as aplicações executadas e o impacto que têm no comportamento geral do sistema.No Modo Intermédio, ao clicar numa aplicação, é apresentado o histórico de utilização de CPU e memória, assim como o nome e o caminho da instalação.

Estas são as funções principais:

- Para proporcionar uma perspectiva da configuração do hardware do sistema
- Para mostrar a utilização de CPU e memória através de um conjunto de indicadores
- Para determinar a utilização de recursos de aplicações
- Para ajudar a fechar qualquer aplicação com elevado consumo de recursos e que esteja a causar o mau desempenho do seu sistema.

Nota
No separador Optimização, no Modo Avançado, sempre que o sistema está inactivo durante um determinado período de tempo, pode iniciar diferentes tipos de análise.

A configuração do sistema é avaliada de acordo com uma classificação do sistema baseada na quantidade de memória RAM instalada, na frequência de CPU e no espaço livre no disco rígido.

No caso de encontrar um problema de abrandamento, este poderá ser causado por algumas aplicações executadas no seu sistema.Para resolver este problema, identifique a aplicação que está na origem e feche-a com a hiperligação fornecida.

Atenção
Se suspeitar que uma aplicação (ou um processo) que pretende fechar faz parte do sistema operativo do Windows e que a sua acção pode afectar o sistema, contacte o Apoio ao Cliente da BitDefender para mais informações.

27. Modo de Jogo / Portátil

O módulo do modo de Jogo / Portátil permite-lhe configurar os modos especiais de operação do BitDefender.

- O Modo de Jogo modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema enquanto estiver a jogar.
- O Modo de Portátil evita que as atrefas agendadas sejam executadas quando o seu portátil esteja em modo de bateria de forma a economizar a mesma.
- Modo Silêncio modifica temporariamente as definições do produto para minimizar as interrupções quando vê filmes ou apresentações.

27.1. Modo de Jogo

O Modo de Jogo modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema.Quando liga o Modo de Jogo, as seguintes definições são aplicadas:

- Todos os alertas e pop-ups do BitDefender são desactivados.
- O nível da protecção em tempo-real do BitDefender é definida como **Permissivo**.
- A Firewall BitDefender está definida para **Permitir todos**.Isto significa que todas as novas ligações (quer de entrada quer de saída) são automaticamente autorizadas, independentemente da porta e do protocolo utilizado.
- As actualizações não são executadas por defeito.

Nota
Para mudar esta definição, clique em Actualização >Configuração e limpe a caixa **Não actualizar se o Modo de Jogo estiver ligado**.

- As tarefas de backup agendadas são desactivadas por defeito.

Por defeito, o BitDefender entra automaticamente em Modo de Jogo quando inicia um jogo da lista dos jogos conhecidos do BitDefender ou quando uma aplicação entra em Modo de ecrã inteiro.Pode entrar manualmente em Modo de Jogo usando a tecla de atalho predefinida `Ctrl+Alt+Shift+G`.É fortemente recomendado que saia do Modo de Jogo quando acaba de jogar (Pode usar a mesma tecla de atalho predefinida `Ctrl+Alt+Shift+G`).

Nota
Enquanto no Modo de Jogo, pode ver a letraG sobre o icone do BitDefender.

Para configurar o Modo Jogo:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá ao **Modo Jogo/Portátil > Modo Jogo**.

No topo da secção, pode ver o estado do Modo de Jogo.Pode clicar em **Modo Jogo está activado** ou **Modo Jogo está desactivado** para alterar o estado actual.

27.1.1. Configurar Modo de Jogo Automático

O Modo de Jogo Automático permite que o BitDefender entre automaticamente em Modo de Jogo quando um jogo é detectado.Pode configurar as seguintes opções:

- **Usar por defeito a lista de jogos do BitDefender** - para entrar automaticamente em Modo de Jogo quando inicia um jogo da lista dos jogos conhecidos do BitDefender.Para ver esta lista, cique em **Gerir Jogos** e depois em **Lista de Jogos**.
- **Acção em Ecrã Completo** - pode escolher activar automaticamente o Modo Jogo ou o Modo Silêncio sempre que uma aplicação fica em ecrã completo.
- **Perguntar se a aplicação em ecrã completo deve ser adicionada à lista de jogos** - para ser notificado para adicionar a nova aplicação à lista de jogos quando deixar o modo de ecrã inteiro.Ao adicionar uma nova aplicação à lista de jogos, da próxima vez que o jogar o BitDefender entrará automaticamente em Modo de Jogo.

Nota
Se não deseja que o BitDefender entre automaticamente em Modo Jogo, desmarque a caixa **Modo de Jogo Automático está activado**.

27.1.2. Gerir a Lista de Jogos

O BitDefender entra automaticamente em Modo de Jogo quando inicia uma aplicação que se encontra na lista de jogos.Para ver e gerira a lista de jogos, clique em **Gerir Jogos**.Uma nova janela irá aparecer.

Novas aplicações são adicionadas automaticamente à lista quando:

- Inicia um jogo da lista de jogos conhecidos do BitDefender.Para ver esta lista, clique em **Lista de Jogos**.
- Após siar do modo de ecrã inteiro, pode adicionar a aplicação à lista de jogos a partir da janela de notificação.

Se deseja descativar o Modo de Jogo Automático para uma determinada aplicação da lista, limpe a correspondente caixa de selecção.Deve de desactivar o Modo de Jogo Automático para as aplicações que regularmente entram em modo de ecrã inteiro, tais como os exploradores da Internet e os leitores de filmes.

Para gerir a lista de jogos, pode usar os botões colocados no topo da tabela:

- **Adicionar** - adiciona uma nova aplicação à lista de jogos.
- **Remover** - remove uma aplicação da lista de jogos.
- **Editar** - edita uma entrada existente na lista de jogos.

27.1.3. Adicionar ou Editar Jogos

Quando adicionar ou editar uma entrada da lista de jogos, aparecerá uma nova janela.

Clique em **Explorar** para seleccionar a aplicação e o caminho da mesma no campo de edição.

Se não quiser entrar automaticamente em Modo de Jogo quando a aplicação seleccionada é executada seleccione **Desactivar**.

Clique em **OK** para adicionar a entrada à lista de jogos.

27.1.4. Configurar as Definições do Modo de Jogo

Para configurar o comportamento das tarefas agendadas, use estas opções:

- **Activar este módulo para modificar os agendamentos das tarefas de análise Antivírus** - evita que a tarefa de análise agendada se execute enquanto o Modo de Jogo estiver ligado.Pode seleccionar uma das seguintes opções:

Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.
Adiar Tarefa	Executa a tarefa imediatamente após sair do Modo de Jogo.

- **Tarefa de Backup** - evita que a tarefa de backup agendada se execute enquanto o Modo de Jogo estiver ligado.Pode seleccionar uma das seguintes opções:

Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.
Adiar Tarefa	Executa a tarefa imediatamente após sair do Modo de Jogo.

Para desactivar automaticamente a firewall BitDefender enquanto estiver no Modo de Jogo, siga os seguintes passos:

1. Clique em **Configuração Avançada**.Uma nova janela irá aparecer.
2. Seleccione a caixa de selecção **Definir Firewall em Permitir Todas (Modo de Jogo) quando em Modo de Jogo**.
3. Clique em **Aplicar** para guardar as alterações.

27.1.5. Mudar a Tecla de Atalho do Modo de Jogo

Pode activar manualmente o Modo Jogo através de`Ctrl+Alt+Shift+G`tecla de atalho.Se deseja mudar a tecla de atalho, siga estes passos:

1. Clique em **Configuração Avançada**.Uma nova janela irá aparecer.
2. Por baixo da opção **Usar Tecla de Atalho** , defina a tecla de atalho desejada:
   - Escolha as teclas que deseja usar ao seleccionar uma das seguintes: Tecla Control (`Ctrl`), Tecla Shift (`Shift`) ou tecla Alternate (`Alt`).
   - No campo de edição, insira a letra correspondente à tecla que deseja usar.

   Por exemplo, de deseja usar as teclas de atalho `Ctrl+Alt+D` , deve seleccionar `Ctrl` e `Alt` e inserir `D`.

   Nota
   Remover a selecção junto a **Activar Tecla de Atalho** irá desactivar a tecla de atalho.

3. Clique em **Aplicar** para guardar as alterações.

27.2. Modo Portátil

O Modo de Portátil foi especialmente desenhado para os utilizadores de portáteis. O seu propósito é minimizar o impacto do BitDefender no consumo de energia enquanto o portátil estiver a funcionar a bateria.

Enquanto estiver em Modo de Portátil, as tarefas agendadas não serão levadas a cabo por defeito.

O BitDefender detecta quando o seu portátil está a funcionar a bateria e automaticamente entra em Modo de Portátil.De igual forma, O BitDefender sai automaticamente do Modo de Portátil quando detecta que o seu portátil já não está a funcionar a bateria.

Para configurar o Modo Portátil:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá ao **Modo Jogo/Portátil > Modo Portátil**.

Pode ver se o Modo de Portátil está ou não ligado.Se o Modo de Portátil está ligado, o BitDefender aplicará as definições configuradas para o portátil a funcionar a bateria.

27.2.1. Configurar Definições do Modo de Portátil

Para configurar o comportamento das tarefas agendadas, use estas opções:

- **Activar este módulo para modificar os agendamentos das tarefas de análise Antivírus** - evita que a tarefa de análise agendada se execute enquanto o Modo de Portátil estiver ligado.Pode seleccionar uma das seguintes opções:

Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.
Adiar Tarefa	Executar a tarefa agendada assim que sair do Modo de Portátil.

- **Tarefa de Backup** - evita que a tarefa de backup agendada se execute enquanto o Modo de Portátil estiver ligado.Pode seleccionar uma das seguintes opções:

Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.
Adiar Tarefa	Executar a tarefa agendada assim que sair do Modo de Portátil.

27.3. Modo Silêncio

O Modo Silêncio modifica temporariamente as definições da protecção de forma a minimizar o seu impacto no desempenho do sistema.Quando liga o Modo Silêncio, as seguintes definições são aplicadas:

- Todos os alertas e pop-ups do BitDefender são desactivados.
- A Firewall BitDefender está definida para **Permitir todos**.Isto significa que todas as novas ligações (quer de entrada quer de saída) são automaticamente autorizadas, independentemente da porta e do protocolo utilizado.
- As tarefas de análise agendadas são desactivadas por defeito.
- As tarefas de backup agendadas são desactivadas por defeito.

Por defeito, o BitDefender activa automaticamente o Modo Silêncio sempre que vê um filme ou uma apresentação ou quando uma aplicação fica no modo de ecrã completo.É vivamente recomendado que saia do Modo Silêncio quando terminar o filme ou a apresentação.

Nota
No Modo Silêncio, pode ver uma ligeira modificação do pequeno ícone do BitDefender localizado junto ao relógio do seu computador.

Para configurar o Modo Silêncio:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá ao **Modo Jogo/Portátil > Modo Silêncio**.

No cimo da secção, pode ver o estado do Modo Silêncio.Pode clicar em **Modo Silêncio está activado** ou **Modo Silêncio está desactivado** para alterar o estado actual.

27.3.1. Configurar a Acção em Ecrã Completo

Pode configurar as seguintes opções:

- **Acção em Ecrã Completo** - pode escolher activar automaticamente o Modo Jogo ou o Modo Silêncio sempre que uma aplicação fica em ecrã completo.

Nota

Se não deseja que o BitDefender entre automaticamente em Modo Silêncio, desmarque a caixa de selecção **Acção em Ecrã Completo**.

27.3.2. Configurar as Definições do Modo Silêncio

Para configurar o comportamento das tarefas agendadas, use estas opções:

- **Activar este módulo para modificar os agendamentos das tarefas de análise Antivírus** - evita que a tarefa de análise agendada seja executada com o Modo Silêncio activado.Pode seleccionar uma das seguintes opções:

Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.
Adiar Tarefa	Executar a tarefa agendada imediatamente após sair do Modo Silêncio.

- **Activar este módulo para modificar tarefas de Backup agendadas** - evita que a tarefa de backup agendada se execute enquanto o Modo Silêncio estiver activado.Pode seleccionar uma das seguintes opções:

Opção	Descrição
Saltar Tarefa	Não executar de todo a tarefa agendada.
Adiar Tarefa	Executar a tarefa agendada imediatamente após sair do Modo Silêncio.

28. A Sua Rede

O módulo de rede permite-lhe gerir os produtos BitDefender instalados nos seus computadores em casa a partir de um só computador.Para aceder ao módulo de Rede Doméstica, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Rede**.

Modo Avançado
: Vá a **Rede Doméstica**.

Nota
Também pode adicionar um atalho a Meus Instrumentos.

Para poder gerir os produtos BitDefender instalados nos computadores de casa, siga os seguintes passos:

1. Activar a rede doméstica do BitDefender no seu computador.Defina o seu computador como Servidor.
2. Vá a cada computador que deseja gerir e adira-o à rede (defina a palavra-passe).Definir cada computador como Normal.
3. Volte para o seu computador e adicione os computadores que deseja gerir.

28.1. Activar a Rede BitDefender

Para activar a rede doméstica do BitDefender, siga os seguintes passos:

1. Clique em **Activar Rede**.Será notificado para configurar a palavra-passe de gestão de rede pessoal.
2. Insira a mesma palavra-passe em cada um dos campos editáveis.
3. Defina a função do computador na rede doméstica do BitDefender:
   - **Computador Servidor** - seleccione esta opção no computador que será utilizado para gerir os outros computadores.
   - **Computador Normal** - seleccione esta opção nos computadores que serão geridos pelo Computador Servidor.
4. Clique em **OK**.

Pode ver o nome do computador a aparecer no mapa de rede.

Aparece o botão **Desactivar Rede**.

28.2. Adicionar Computadores à Rede BitDefender

Todos os computadores serão automaticamente adicionados à rede se cumprir os seguintes requisitos:

- a rede doméstica BitDefender foi activada nele.
- a função foi definida como Computador Normal.
- a palavra-passe definida na activação da rede é a igual à definida no Computador Servidor.

Nota
No Modo Avançado, pode analisar a rede doméstica para encontrar os computadores que cumprem os requisitos clicando no botão **Auto-descobrir**.

Para adicionar manualmente um computador à rede doméstica BitDefender a partir do Computador Servidor, siga os seguintes passos:

1. Clique em **Adicionar Computador**.
2. Insira a palavra-passe de gestão rede pessoal e clique em **OK**.Uma nova janela irá aparecer.

   Pode ver a lista dos computadores na rede.O significado do ícone é o seguinte:

   Indica um computador on-line sem produtos BitDefender instalados.
   Indica um computador on-line com o BitDefender instalado.
   Indica um computador offline com o BitDefender instalado.
3. Faça uma das coisas seguintes:
   - Seleccione da lista o nome do computador a adicionar.
   - Insira o endereço IP ou o nome do computador a adicionar no campo correspondente.
4. Prima **Adicionar**.Será notificado para inserir a sua palavra-passe de gestão de rede pessoal do respectivo computador.
5. Insira a palavra-passe de gestão de rede pessoal configurada no respectivo computador.
6. Clique em **OK**.Se forneceu a palavra-passe correcta, a nome do computador seleccionado aparecerá no mapa de rede.

28.3. Gerir a Rede BitDefender

Uma vez que tenha criado com sucesso a sua rede pessoal BitDefender pode gerir todos os produtos BitDefender a partir de um único computador.

Se mover o curso do seu rato sobre um computador do mapa de rede, pode ver alguma informação acerca dele (nome, endereço IP, número de incidências que estão a afectar a segurança do sistema, o estado de registo do BitDefender).

Se clicar botão direito do rato sobre o nome de um computador no mapa de rede, pode ver todas as tarefas administrativas que pode levar a cabo no computador remoto.

- **Registar o BitDefender neste computador**

  Permite-lhe registar o BitDefender neste computador introduzindo a chave de licença.

- **Definir palavra-passe para acesso às definições num computador remoto**

  Permite-lhe criar uma password para restringir o acesso às definições do BitDefender nestes PC.

- **Executar tarefa de análise a-pedido**

  Permite-lhe executar uma análise a-pedido remota a partir de outro computador. Pode efectuar uma das seguintes tarefas: Análise Os Meus Documentos, Análise Completa do Sistema e Análise Minunciosa do Sistema.

- **Reparar incidências neste computador**

  Permite-lhe reparar as incidências que estão a afectar a segurança deste computador seguindo o assistente Reparar Incidências.

- **Ver Histórico/Eventos**

  Permite-lhe aceder ao módulo **Histórico&Eventos** do produto BitDefender instalado neste computador.

- **Actualizar Agora**

  Inicia o processo de Actualização para o produto BitDefender installado neste computador.

- **Definir Perfil de Controlo Parental**

  Permite-lhe definir as categorias de faixas etárias a serem utilizadas pelo filtro de Internet do Controlo Parental neste computador.

- **Levar a cabo uma tarefa de Optimização neste computador**

  Permite-lhe correr uma tarefa de Optimização através de um computador remoto. Possibilita uma das seguintes tarefas: desfragmentação do disco ou a limpeza dos ficheiros temporários de Internet.

- **Definir com Servidor de Actualização desta rede**

  Permite-lhe definir este computador como servidor de actualizações para todos os produtos BitDefender instalados nos computadores desta rede.A utilização

desta opção reduz o trafego de internet, porque apenas um computador vai necessitar de aceder a internet para descarregar as actualizações.

- **Remover o PC desta rede pessoal**

  Permite-lhe remover um PC da Rede.

Se o interface do BitDefender estiver no Modo Intermédio, pode executar várias tarefas em todos os computadores geridos ao mesmo tempo clicando nos respectivos botões.

- **Analisar Todos** - permite-lhe analisar ao mesmo tempo todos os computadores geridos.
- **Actualizar Todos** - permite-lhe actualizar ao mesmo tempo todos os computadores geridos.
- **Registar Todos** - permite-lhe registar ao mesmo tempo todos os computadores geridos.

Antes de levar a cabo uma tarefa num computador específico, será notificado para inserir a palavra-passe de gestão de rede pessoal local.Insira a palavra-passe de gestão rede pessoal e clique em **OK**.

Nota

Se planeia levar a cabo várias tarefas, seleccione **Não me mostrem mais esta mensagem durante esta sessão**.Ao seleccionar esta opção, não será notificado novamente pela palavra-passe durante esta sessão.

29. Actualização

Todos os dias é encontrado e identificado novo malware. Esta é a razão pela qual é muito importante manter o BitDefender actualizado com as últimas assinaturas de malware.

Se está ligado à Internet através de banda larga ou ADSL, o BitDefender executa esta operação sozinho. Quando liga o computador o BitDefender verifica se há novas actualizações e depois disso fá-lo a cada **hora** .

Se uma actualização é detectada, poderá ser notificado para confirmar a actualização ou a mesma é levada a cabo automaticamente, dependendo das definições automáticas da actualização.

O processo de actualização é executado "on the fly", o que significa que os ficheiros são substituidos progressivamente. Desta forma, o processo de actualização não afectará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

Importante

Para estar protegido contra as mais recentes ameaças mantenha a **Actualização Automática** activada.

As actualizações vêm em quatro “sabores”:

- **Actualizações para a engenharia Antivírus** - à medida que vão surgindo novas ameaças, os ficheiros que contêm assinaturas de vírus têm de ser actualizados para assegurar a protecção actualizada permanente contra os vírus. Esta actualização é também conhecida como **Virus Definitions Update**.
- **Actualizações para a engenharia Antispam** - novas regras serão adicionadas ao Filtro Heurístico e ao Filtro URL e filters novas assinaturas de imagens serão adicionadas ao Filtro de Imagem. Isto irá a judar a melhorar a eficiência da sua engenharia Antispam. Esta actualização é também conhecida como **Antispam Update**.
- **Actualizações para o motor de Antispyware** - novas assinaturas de spyware serão adicionadas à base de dados. Esta actualização é também conhecida como **Antispyware Update**.
- **Actualizações do produto** - quando é lançada uma nova versão do produto, são introduzidas novas configurações e técnicas de verificação, com o objectivo de melhorar o desempenho do produto. Esta actualização é também conhecida como **Product Update**.

29.1. Efectuar uma Actualização

A actualização automática pode também ser feita a qualquer altura que deseje premindo o botão **Actualizar Agora**. Esta actualização é também conhecida como **actualização a pedido do utilizador**.

Para actualizar o BitDefender, consoante o modo do interface, proceda da seguinte forma:

Modo Básico
Clique no ícone **Actualizar Agora** na área Proteja o seu PC.

Modo Intermédio
Abra o separador **Segurança** e clique em **Actualizar Agora**, nas Tarefas Rápidas, no lado esquerdo da janela.

Modo Avançado
Vá a **Actualizar > Actualizar**.

O módulo de **Actualização** estabelece ligação ao servidor de actualizações do BitDefender e verificará se há actualizações disponíveis. Se detectar uma actualização, dependendo das opções definidas na secção Opções da Actualização Manual, ser-lhe-á solicitada a confirmação para a actualização ou a actualização será feita automaticamente.

Importante
Poderá ser necessário reiniciar o computador quando a actualização tiver terminado. Recomendamos que o faça o quanto antes.

Nota

Se está ligado à Internet através de uma ligação dial-up, então é uma boa ideia adquirir o hábito de actualizar o Bitdefender a seu pedido.Para mais informação, por favor consulte o *“Como Actualizar o BitDefender numa Ligação à Internet Lenta”* (p. 234).

29.2. Configurar Definições de Actualização

As actualizações podem ser executadas através da rede local, da Internet, directamente ou através de um servidor proxy.Por defeito, o BitDefender verificará as actualizações a cada hora, via Internet, e instalará as que estejam disponíveis sem o avisar.

Para configurar as definições de actualização:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Actualização > Definições**.

3. Configure as definições como necessário.Para saber o que uma opção faz, mantenha o rato sobre a mesma e leia a descripção apresentada no fundo da janela.
4. Prima **Aplicar** para guardar as alterações.

Para aplicar as configurações por defeito, clique em **Por Defeito**.

As configurações da actualização estão agrupadas em 4 categorias (**Configuração da Localização da Actualização**, **Configuração de actualização automática**, **Configuração de Actualização Manual** e **Configuração Avançada**). Cada categoria será descrita separadamente.

29.2.1. Configuração da Localização da Actualização

Para definir a localização da actualização, use as opções da categoria **Configuração da Localização da Actualização** .

Nota

Configure estas definições apenas se estiver ligado a uma rede local que armazena localmente as assinaturas de malware do BitDefender ou se liga à Internet através de um servidor proxy.

Para actualizações mais rápidas e fiáveis, pode configurar dois locais de actualização: um **Local primário de actualização** e um **Local alternativo de actualização**. Por defeito estas localizações são iguais:`http://upgrade.bitdefender.com`.

Para modificar um dos locais de actualização, insira o URL do local mirror no campo **URL** que corresponde ao novo local para o qual deseja mudar.

Nota

Recomendamos que defini como local primário de actualização o local mirror e deixar o local alternativo de actualização como está, como um plano de backup em caso do local mirror ficar indisponível.

No caso em que a empresa usa um servidor proxy para se ligar à Internet, seleccione **Usar proxy** de depois clique em **Gerir proxies** para configurar as definições do proxy.Para mais informações, por favor consulte“Definições de Ligação” (p. 61)

29.2.2. Configurar Actualização Automática

Para configurar o processo de actualização automática do BitDefender, use as opções na categoria **Configuração Actualização Automática** .

Pode definir o intervalo entre duas verificações consecutivas de actualizações no campo **Intervalo de Tempo**. Por defeito, o intervalo de tempo da actualização é de 1 hora.

Para definir como é que o processo de actualização automática tem de ser feito, seleccione uma das seguintes opções:

- **Actualização silenciosa** - O BitDefender faz automaticamente o download e a implementação da actualização.
- **Avisar antes de fazer download das actualizações** - cada vez que uma actualização está disponível, será consultado antes do download ser feito.
- **Avisar antes de instalar actualizações** - cada vez que uma actualização for descarregada, será consultado antes da sua instalação ser feita.

29.2.3. Configurar Actualização Manual

Para definir como a actualização manual (actualização a pedido do utilizador) deve ser executada, seleccione uma das seguintes opções na categoria **Configuração Actualização Manual**:

- **Actualização silenciosa** - a actualização manual será feita em segundo plano automaticamente.
- **Avisar antes de fazer download das actualizações** - cada vez que uma actualização está disponível, será consultado antes do download ser feito.

29.2.4. Configuração Avançada

Para evitar que o processo de actualização do BitDefender interfira com o seu trabalho, configure as opções na categoria **Configuração Avançada**:

- **Esperar pelo reiniciar, em vez se o solicitar** - Se uma actualização requer um reiniciar, o produto continuará a funcionar com os antigos ficheiros até que o sistema reinicie. Ao utilizador não lhe será solicitado que o reinicie, logo o processo de actualização do BitDefender não interferirá com o trabalho do utilizador.
- **Não actualizar se a análise estiver a decorrer** - O BitDefender não vai actualizar se estiver a decorrer uma análise. Desta forma, o processo de actualização do BitDefender não vai interferir com as tarefas de análise.

Nota

Se o BitDefender for actualizado enquanto a análise estiver a decorrer, o processo de análise será interrompido.

- **Não actualizar se o Modo Jogo estiver activado** - O BitDefender não actualizará se o Modo Jogo estiver activado.Desta forma, poderá minimizar a influência do produto no desempenho do sistema durante os jogos.
- **Activar partilha de actualizações** - Se quiser minimizar o impacto do tráfego de rede no desempenho do sistema durante as actualizações, utilize a opção de partilha de actualizações.
- **Transferir ficheiros do BitDefender deste PC** - O BitDefender permite-lhe partilhar as mais recentes assinaturas antivírus disponíveis no seu computador com outros utilizadores do BitDefender.

Como

30. Como Posso Analisar Ficheiros e Pastas?

A análise é simples e flexível com o BitDefender.Há várias formas de definir o BitDefender para analisar ficheiros e pastas em busca de vírus e outro malware:

- Usar o Menu Contextual do Windows
- Usar Tarefas de Análise
- Usando a Barra de Actividade da Análise

Uma vez que inicie uma análise, o assistente de Análise de Antivírus irá aparecer e guiá-lo através do processo de análise.Para mais informações sobre este assistente, por favor consulte o "*Assistente de Análise Antivírus*" (p. 73).

Nota

Para saber como utilizar o BitDefender para analisar no Modo de Segurança do Windows, consulte "*Como Posso Analisar o Computador no Modo de Segurança?*" (p. 248).

30.1. Usar o Menu Contextual do Windows

Esta é a forma mais fácil e recomendada para analisar um ficheiro ou pasta no seu computador.Clique com o botão direito do rato sobre o objecto que pretende analisar e seleccione no menu **Analisar com o BitDefender**.Siga o assistente de Análise Antivírus para completar a análise.

Situações tipicas em que deve de usar este método de análise são as seguintes:

- Suspeita que um determinado ficheiro ou pasta está infectado.
- Sempre que descarrega da Internet ficheiros que julga serem perigosos.
- Quer analisar uma partilha de rede antes de copiar os ficheiros para o seu computador.

30.2. Usar Tarefas de Análise

Se deseja analisar o seu computador ou determinadas pastas regularmente, deve de considerar usar as tarefas de análise.Tarefas de análise indicam ao BitDefender as áreas a analisar, e que opções ou acções de análise devem ser usadas. Mais ainda, pode Agendá-las para serem levadas a cabo numa base regular ou numa determinada altura.

Para analisar o seu computador usando as tarefas de análise, deve de abrir o interface BitDefender e levar a cabo a tarefa de análise desejada.Dependendo do modo do interface do utilizador, são várias as etapas a seguir para executar o scan.

Levar a cabo Tarefas de Análise em Modo Básico

No Modo Básico, pode executar várias tarefas de análise pré-configuradas.Clique no botão **Segurança** e escolha a tarefa de análise pretendida.Siga o assistente de Análise Antivírus para completar a análise.

Realizar Tarefas de Análise em Modo Intermédio

Na Modo Intermédio, pode executar várias tarefas de análise pré-configuradas. Também pode configurar e executar tarefas de análise personalizadas especificando as localizações nas opções de análise.Siga estes passos para realizar uma tarefa de análise em Modo Intermédio:

1. Clique na barra **Segurança** .
2. No lado esquerdo da área de Tarefas Rápidas, clique em **Análise Minuciosa ao Sistema** e escolha a tarefa de análise pretendida.Para configurar e executar uma anákise personalizada, clique em **Análise Personalizada**.
3. Siga o assistente de Análise Antivírus para completar a análise.Se preferir executar uma análise personalizada, deverá completar o assistente de Análise Personalizada.

Executar Tarefas de Análise em Modo Avançado

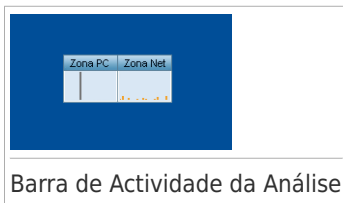
No Modo Avançado, pode levar a cabo todas as tarefas de análise pré-configuradas, e também alterar as suas opções. Mais ainda, pode criar as suas próprias tarefas de análise se deseja analisar locais específicos no seu computador.Siga estes passos para realizar uma tarefa de análise em Modo Avançado:

1. Clique em **Antivirus** do lado esquerdo do menu.
2. Clique na barra **Analisar**Aqui pode encontrar um conjunto de tarefas de análise pré-configuradas e pode criar as suas próprias tarefas de análise.
3. Faça duplo-clique na tarefa de análise que quer executar.
4. Siga o assistente de Análise Antivírus para completar a análise.

30.3. Usando a Barra de Actividade da Análise

A **Barra de Actividade da Análise** é um gráfico de visualização da actividade de verificação no seu sistema.Esta pequena janela, por defeito, está apenas disponível no Modo Avançado.

Barra de Actividade da Análise

Pode usar a barra de actividade da análise para analisar rapidamente ficheiros e pastas.Drag & drop o ficheiro ou pasta a ser analisado para a

barra de actividade da análise.Siga o assistente de Análise Antivírus para completar a análise.

Nota

Para mais informação, por favor consulte o “*Barra de Actividade da Análise*” (p. 21).

31. Como Posso Criar Uma Tarefa de Análise Personalizada?

Para criar uma tarefa de análise, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio

Abra o separador **Segurança** e clique em **Personalizar Análise**, nas Tarefas Rápidas, no lado esquerdo da janela.

Vai aparecer um assistente para ajudar a criar uma tarefa de análise.Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**.Para sair do assistente, clique em **Cancelar**.

1. **Bem-vindo**
2. **Seleccionar Alvo**

   Clique em **Adicionar Alvo** para seleccionar os ficheiros ou as pastas a analisar.

   Clique em **Configuração Avançada**.No separador **Apresentação**, configure as opções de análise movendo o cursor na barra deslizante.Se desejar configurar detalhadamente as opções de análise, clique em **Personalizar**.Abra o separador **Agendar** para escolher quando a tarefa deve ser executada.
3. **Terminar**

   Aqui pode inserir o nome da tarefa e, opcionalmente, adicionar a análise na área das Tarefas Rápidas.

   Clique em **Iniciar Análise** para criar a tarefa e iniciar o assistente de análise.

Modo Avançado

1. Vá a **Antivírus > Análise de Vírus**.
2. Clique em **Nova Tarefa**Aparecerá uma nova janela.

   Nota

   Também pode clicar com o botão direito numa tarefa de análise predefinida, como a **Análise Minuciosa ao Sistema** e escolher **Clonar Tarefa**.Isto é útil na criação de novas tarefas, pois pode modificar as definições da tarefa duplicada.
3. No separador **Apresentação**, introduza o nome da tarefa e configure as opções de análise movendo o cursor na barra deslizante.

Se desejar configurar detalhadamente as opções de análise, clique em **Personalizar**.

4. Vá ao separador **Caminhos** para seleccionar o alvo da análise. Clique em **Adicionar Itens** para seleccionar os ficheiros ou as pastas a analisar.
5. Abra o separador **Agendar** para escolher quando a tarefa deve ser executada.
6. Clique em **Ok** para guardar a tarefa.A nova tarefa vai aparecer nas tarefas definidas pelo Utilizador e pode ser editada, removida ou executada em qualquer momento a partir desta janela.

32. Como Posso Agendar uma Análise ao Computador?

Analisar o seu computador periodicamente é a melhor prática para o manter livre de malware. O BitDefender permite-lhe agendar as tarefas de análise de forma a poder analisar automaticamente o seu computador.

Para agendar o BitDefender de forma a analisar o seu computador, siga estes passos:

1. Abrir o BitDefender.
2. Dependendo do modo de interface do utilizador, proceda da seguinte forma:

   Modo Intermédio
   : Abra o separador **Segurança** e clique em **Configurar o Antivírus**, nas Tarefas Rápidas, no lado esquerdo da janela.

   Modo Avançado
   : Clique em **Antivirus** do lado esquerdo do menu.
3. Clique na barra **Analisar**Aqui pode encontrar um conjunto de tarefas de análise pré-configuradas e pode criar as suas próprias tarefas de análise.
   - As tarefas de sistema estão disponíveis e podem ser levadas a cabo em qualquer conta de utilizador Windows.
   - Tarefas de utilizador estão apenas disponíveis para o mesmo e só podem ser usadas por quem as criou.

   Estas são as análises pré-configuradas que pode agendar:

   Análise Completa
   : Analisa todo o sistema, excepto arquivos.Na configuração por defeito, analisa todos os tipos de malware excepto rootkits.

   Análise Rápida
   : A Análise Rápida utiliza a análise nas nuvens para detectar malware em execução no seu sistema.Normalmente, a realização de uma Análise Rápida demora menos de um minuto e utiliza uma facção dos recursos do sistema necessários para uma análise de vírus normal.

   Análise Autologon
   : Analisar os itens que são executados quando o utilizador entra no Windows.Para usar esta tarefa, deve de agendá-la para ser levada a cabo durante o iniciar do sistema.Por defeito, a análise ao logon está desactivada.

   Análise Minuciosa
   : Analisa todo o sistema.Na configuração por defeito, faz uma nálise em busca de todo o tipo de malware que ameaçe a segurança do seu sistema, tais como vírus, spyware, adware, rootkits e outros.

Os meus documentos

Use esta tarefa para analisar pastas de utilizadores actuais: `Os Meus Documentos`, `Ambiente de Trabalho` e `StartUp`. Isto irá assegurar a segurança dos seus documentos, uma área de trabalho segura e aplicações limpas a serem executadas no arranque.

Se nenhuma destas tarefas de análise servir, pode criar uma nova tarefa de análise que pode depois agendar para ser levada a cabo quando quiser.

4. Clique com o botão-direito na tarefa de análise desejada e seleccione **Agendar**.Uma nova janela irá aparecer.
5. Agende a tarefa para ser levada a cabo quando quiser:
   - Para levar a cabo a tarefa de análise uma só vez, seleccione **Uma só vez** e especifique a data e hora de inicio.
   - Para levar a cabo a tarefa de análise após o iniciar do sistema, seleccione **No iniciar do sistema**.Pode definir quanto tempo após o iniciar do sistema a tarefa deve de ser iniciada.
   - Para levar a cabo a tarefa de análise numa base regular, seleccione **Periodicamente** e especifique a frequência e a data e hora de inicio.

Nota

Por exemplo, para analisar o seu computador cada Sábado às 2 PM, deve de configurar o agendar da seguinte forma:

a. Seleccione **Periodicamente**.

b. No campo **A cada**, insira 1 e depois seleccione **semanas** do menu.Desta forma, a tarefa é levada a cabo a cada semana.

c. Defina como data de início o primeiro Sábado a aparecer.

d. Defina como hora de início `2:00:00 AM`.

6. Clique em **OK** para guardar o agendamento.A tarefa de análise irá ser levada a cabo automaticamente de acordo com o agendamento que definiu.Se o computador estiver desligado durante o momento do agendamento, a tarefa será levada a cabo da próxima vez que iniciar o seu computador.

33. Como Posso Fazer Cópias de Segurança?

Com o BitDefender Total Security 2011, pode fazer cópias de reserva dos seus dados mais valiosos (documentos, imagens, etc) em vários suportes:

- o seu computador
- Um dispositivo de armazenamento USB
- a localização de uma rede
- CD/DVD
- Um servidor FTP

Uma cópia de segurança ajuda-o a proteger-se contra a perda de dados.Se fizer regularmente cópias de segurança dos seus dados, poderá restaurá-los quando necessário.Desta forma, poderá recuperar ficheiros perdidos ou voltar a versões anteriores de um documento.

Importante
O BitDefender Total Security 2011 não foi concebido para fazer backup e restaurar o Windows. Não pode criar uma imagem do sistema operativo e das aplicações instaladas de modo a que possa restaurar mais tarde o seu sistema para que o estado, se necessário.

Para fazer o backup de dados de um suporte de armazenamento local, siga estes passos:

1. Abrir o BitDefender.
2. Iniciar o assistente de backup local.
   - No Modo Intermédio, abra o separador **Armazenamento de Ficheiros**, clique em **Backup Local** e seleccione **Backup Local**.
   - No Modo Avançado, vá a **Backup** e clique em **Backup Local**.
3. Siga os seguintes passos do assistente para configurar e criar o backup.Para mais informações, por favor consulte “*Fazer o Backup Local de Dados*” (p. 148).
   a. Clique **Seguinte**.
   b. Seleccione os dados que quer fazer backup e clique em **Seguinte**.
   c. Especifique onde quer fazer o backup dos dados seleccionados: seleccione um meio de armazenamento, clique em **Explorar** e escolha a localização do backup (excepto se fizer o backup num CD/DVD).Clique **Seguinte**.
   d. Configure um agendamento de backup se necessário, e clique **Seguinte**.
   e. Defina um nome para a tarefa de backup e clique **Iniciar Backup**.
   f. espere que o backup termine e clique em **Terminar**.

Se precisar de mais opções de backup, ou se quiser gerir as tarefas de backup que criou, abra o BitDefender no Modo Avançado, vá a **Backup** e clique em

Definições.Para mais informações, por favor consulte “*Definições de Backup*” (p. 151).

34. Como Posso Restaurar os Dados da Cópia de Segurança?

Com o BitDefender poderá recuperar facilmente dados perdidos que já tenha feito backup.Antes de restaurar quaisquer dados, assegure-se que o dispositivo onde se encontram os mesmos se encontra disponível.Dependendo do dispositivo que utiliza, poderá necessitar de levar a cabo uma das seguintes acções:

- Inserir a pen USB do backup na porta USB.
- Inserir o CD/DVD do backup na respectiva drive.
- Verifique que é possível ligar-se ao local da rede ou ao servidor FTP onde se encontra armazenado o backup.

Para restaurar dados guardados num dispositivo de armazenamento, estes passos:

1. Abrir o BitDefender.
2. Iniciar o assistente de restauro local.
   - No Modo Intermédio, abra o separador **Armazenamento de Ficheiros**, clique em **Backup Local** e seleccione **Restauro Local**.
   - No Modo Avançado, vá a **Backup** e clique em **Restauro Local**.
3. siga os passos do assistente para recuperar os seus dados.Para mais informações, por favor consulte “*Restaurar Dados de Backup Local*” (p. 150).
   a. Clique **Seguinte**.
   b. Especifique o ficheiro backup de onde deseja restaurar os dados: seleccione o meio de armazenamento, clique em **Explorar** e localize o `.ecs` ficheiro de backup.Clique **Seguinte**.
   c. Especifique as condições de restauro de dados e clique **Seguinte**.Pode escolher restaurar dados para um diferente local ou restaurar dados especificos.
   d. Clique em **Restaurar**.
   e. Espere que o backup termine e clique em **Terminar**.

Se precisar de mais opções de restauro de dados, ou se quiser gerir as tarefas de restauro já criadas, abra o BitDefender no Modo Avançado, vá a **Backup** e clique em **Definições**.Para mais informações, por favor consulte “*Definições de Backup*” (p. 151).

35. Como Posso Criar Contas de Utilizador do Windows?

Uma conta de utilizador do Windows é um perfil exclusivo que inclui todas as definições, os privilégios e os ficheiros pessoais de cada utilizador.

As contas do Windows permitem ao administrador do PC controlar o acesso dos restantes utilizadores.

É muito útil definir contas de utilizador quando o computador é utilizado tanto por adultos como por crianças - um pai pode definir uma conta para cada filho.

Escolha o seu sistema operativo para saber como criar contas do Windows.

- Windows XP:
  1. Inicie sessão no seu computador como administrador.
  2. Clique em Iniciar, Painel de Controlo e, depois, em Contas de Utilizador.
  3. Clique em Criar uma nova conta.
  4. Escreva o nome do utilizador. Pode utilizar o nome completo, o primeiro nome ou um pseudónimo. Depois, clique em Seguinte.
  5. Para o tipo de conta, escolha Limitada e depois seleccione Criar Conta. As contas limitadas são adequadas para crianças pois não permitem fazer alterações ao sistema ou instalar certas aplicações.
  6. A sua nova conta será criada e apresentada no ecrã Gerir Contas.
- Windows Vista ou Windows 7:
  1. Inicie sessão no seu computador como administrador.
  2. Clique em Iniciar, Painel de Controlo e, depois, em Contas de Utilizador.
  3. Clique em Criar uma nova conta.
  4. Escreva o nome do utilizador. Pode utilizar o nome completo, o primeiro nome ou um pseudónimo. Depois, clique em Seguinte.
  5. Para o tipo de conta, escolha Padrão e depois seleccione Criar Conta. As contas limitadas são adequadas para crianças pois não permitem fazer alterações ao sistema ou instalar certas aplicações.
  6. A sua nova conta será criada e apresentada no ecrã Gerir Contas.

Nota
Agira que adicionou novas contas de utilizador, pode criar palavras-passe para as contas.

36. Como Posso Actualizar o BitDefender Através de um Proxy?

Normalmente, o BitDefender detecta e importa automaticamente as definições proxy do seu sistema.Se estiver ligado à Internet através de um servidor proxy, poderá ter de procurar as definições proxy e configurar o BitDefender correctamente.Para saber como fazer isto, consulte "*Como Posso Encontrar as Minhas Definições de Proxy?*" (p. 262).

Depois de encontrar as definições de proxy, siga os seguintes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Geral > Definições**.
3. Clique em **Definições Proxy** na secção**Definições da Ligação**.
4. Insira as definições de proxy nos respectivos campos.
5. Clique em **OK**.

Nota

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção "*Apoio*" (p. 253).

37. Como Posso Fazer o Upgrade para Outro Produto do BitDefender 2011?

Com o BitDefender 2011 pode fazer facilmente o upgrade de um produto BitDefender 2011 para outro.

Tudo o tem de fazer é adquirir uma chave de licença para o BitDefender 2011 que quer fazer o upgrade e introduza-a na janela de registo do produto BitDefender 2011 que está actualmente a utilizar.

Siga estes passos:

1. Abrir o BitDefender.
2. Clique na hiperligação **Informação de Licença** no fundo da janela.A janela de registo irá aparecer.
3. Introduza a chave de registo e clique em **Registar Agora**.
4. O BitDefender irá informar que a chave de licença destina-se a um produto diferente e dará a opção de instalá-lo.Clique na respectiva hiperligação e siga o procedimento de três passos para efectuar o upgrade.

   a. **Confirmar Acção**

   b. **Upgrade em curso**

      Aguarde que o BitDefender conclua o processo de upgrade.Isto irá demorar alguns minutos.

   c. **Upgrade concluído**

      O processo foi concluído. Poderá ser necessário reiniciar o sistema.

38. Como Posso Melhorar a Velocidade do Meu Sistema?

A velocidade do sistema não depende apenas das características do hardware, tais como a capacidade do CPU, a memória disponível e o espaço no disco rígido.Está, também, directamente relacionada com a configuração do software e com a gestão dos dados.

Estas são as acções principais que pode efectuar com o BitDefender para melhorar a velocidade e o desempenho do seu sistema:

- Desfragmentador de Disco reorganiza fisicamente os seus dados no disco rígido para aceder aos ficheiros mais rapidamente e para melhorar o desempenho do sistema.
- O Limpa PC melhora o desempenho do sistema removendo aqueles ficheiros que já não são necessários, por exemplo: ficheiros temporários da Internet, cookies e ficheiros temporários do sistema.
- Limpa Registos analisa o Registo do Windows e elimina as chaves de registo inválidas, melhorando o desempenho do seu sistema.
- Analise o Sistema Periodicamente, pelo menos uma vez por mês para assegurar que a velocidade e as operações do seu sistema não são afectadas por malware.

39. Como Posso Utilizar Cofres de Ficheiros?

O Cofre de Ficheiros BitDefender permite-lhe criar unidades lógicas encriptadas, e protegidas por palavra-passe (cofres) no seu computador onde pode armazenar em segurança os seus documentos confidenciais e sensíveis.Fisicamente, o cofre é um ficheiros armazenado no seu disco rígido local com a extensão .bvd.

Ao criar um cofre de ficheiros, há dois coisas importantes: o tamanho e a palavra-passe.O tamanho predefinido de 50 MB deve ser o suficiente para os seus documentos privados, ficheiros do Excel e outros semelhantes. No entanto, para vídeos ou ficheiros de grandes dimensões, poderá precisar de mais espaço.

Para proteger totalmente os ficheiros ou pastas confidenciais ou sensíveis nos cofres de ficheiros do BitDefender, proceda da seguinte forma:

- **Crie um cofre de ficheiros e defina uma palavra-passe forte para ele.**

  Para criar um Cofre de Ficheiros, clique com o botão direito numa área vazia do ambiente de trabalho ou numa pasta do seu computador, aponte o cursor para Cofre de Ficheiros BitDefender e seleccione **Criar cofre**.

  Aparecerá uma nova janela. Proceda da seguinte forma:

  1. Clique em **Explorar** para seleccionar a localização do cofre e guarde o cofre de ficheiros sob o nome desejado.
  2. Escolha uma letra de drive do menu. Quando abrir o cofre, um disco virtual será etiquetado com a letra seleccionada, aparecendo no **Meu Computador**.
  3. Insira a palavra-passe do cofre nos campos **Palavra-passe** e **Confirmar**.
  4. Se deseja mudar o tamanho por defeito (50 MB) do cofre, insira o valor desejado no campo **Tamanho Cofre** .
  5. Clique em Criar se apenas pretender criar o cofre na localização seleccionada. Para criar e apresentar o cofre como uma unidade de disco virtual no **Meu Computador** clique em **Criar e Abrir**.

  Nota
  Quando abre o cofre, aparece uma unidade de disco virtual no **Meu Computador**. A unidade é assinalada com a letra atribuída ao cofre.

- **Adicione os ficheiros e as pastas que deseja proteger no cofre.**

  Para adicionar um ficheiro a um cofre, tem de abrir o cofre primeiro.

  1. Procure o ficheiro de cofre .bvd.
  2. Clique com o botão direito no ficheiro do cofre, aponte para Cofre de Ficheiros BitDefender e seleccione **Abrir**.

3. Na janela que aparece, seleccione uma letra de unidade para atribuir ao cofre, introduza a palavra-passe e clique em **Abrir**.

   Agora, pode efectuar operações na unidade que corresponde ao cofre de ficheiros pretendido com o Explorador do Windows, tal como faria com qualquer outras unidade.Para adicionar um ficheiro a um cofre aberto, também pode clicar com o botão direito no ficheiro, apontar para o Cofre de Ficheiros BitDefender e seleccione **Adicionar ao cofre de ficheiros**.

- **Mantenha o cofre sempre fechado.**

  Só abra os cofres quando precisar de aceder ou gerir o conteúdo.Para fechar um cofre, clique com o botão-direito do rato no correspondente disco virtual no **Meu Computador**, aponte para **Cofre de Ficheiros BitDefender** e seleccione **Fechar**.

- **Certifique-se que não elimina o ficheiro de cofre .bvd.**

  Eliminar o ficheiro também elimina o conteúdo do cofre.

Para mais informações sobre como trabalhar com cofres de ficheiros, por favor consulte “*Encriptação Ficheiro*” (p. 174).

Troubleshooting e Obter Ajuda

40. Solução de problemas

Este capítulo apresenta alguns dos problemas que poderá encontrar ao utilizar o BitDefender e as possíveis soluções.A maioria destes problemas pode ser resolvida com a configuração correcta das definições do produto.

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da BitDefender como mostrado no capítulo “*Apoio*” (p. 253).

40.1. Problemas de Instalação

Este artigo vai ajuda-lo a solucionar os problemas de instalação mais comums do BitDefender.Estes problemas podem ser agrupados nas seguintes categorias:

- Erros de validação de Instalação: o assistente de configuração não pode ser executado devido a condições específicas do seu sistema.
- Instalações falhadas: iniciou a instalação do assistente de configuração, mas não foi concluída com êxito.

40.1.1. Erros de Validação da Instalação

Quando você iniciar o assistente de instalação, um número de condições são verificadas para validar se a instalação pode ser iniciada.A seguinte tabela apresenta as validadções e erros das instalações mais comuns, bem como o ajuda a solucioná-las.

Erro	Descrição&Solução
Não possui privilégios suficientes para instalar o programa.	Para poder executar o assistente de instalação e instalar o BitDefender necessita de provilégios de administrador.Faça uma das coisas seguintes: ● Entre com uma conta de administrador do Windows e execute de novo o assistente de instalação. ● Clique com o botão-direito no ficheiro de instalação **Executar como**.Digite no sistema o nome de utilizador e a palavra-passe de uma conta de administrador do Windows.
O instalador detectou uma versão anterior do produto BitDefender que não foi devidamente desinstalada.	O BitDefender foi anteriormente instalado no seu sistema, mas a instalação não foi completamente removida. Esta condição bloqueia uma nova instalação do BitDefender.

Erro	Descrição&Solução
	Para superar este erro e instalar o BitDefender, siga estes passos: 1. Vá a www.bitdefender.com/uninstall e descarregue a ferramenta de desinstalação para o seu computador. 2. Execute a ferramenta de desinstalação com direitos de administrador. 3. Reinicie o seu computador. 4. Volte a iniciar o assistente de instalação para reinstalar o BitDefender.
O produto BitDefender não é compatível com o seu sistema operativo.	Está a tentar instalar o BitDefender num sistema operativo nao suportado.Por favor consulte o *"Requisitos de Sistema"* (p. 2) para saber em que sistemas operativos pode instalar no BitDefender. Se o seu sistema operativo é o Windows XP com o Service Pack 1 ou sem nenhum service pack, pode instalar o Service Pack 2 ou superior e em seguida executar novamente o assistente de instalação.
O ficheiro de instalação foi concebido para um diferente tipo de processador.	Se receber esse erro, significa que está a tentar executar uma versão incorreta do ficheiro de instalação.Existem duas versões do ficheiro de instalação do BitDefender: um para processadores 32-bit e outro para processadores 64-bit. Para se certificar que tem a versão correta para o seu sistema, faça o download do ficheiro de instalação diretamente do site www.bitdefender.com.

40.1.2. Falha na Instalação

Existem várias possibilidades para instalação falhar:

- Durante a instalação, aparece uma imagem de erro.Pode ser solicitado que cancele a instalação ou fornecido um botão para executar a ferramenta de desinstalação que irá limpar o sistema.

Nota
Imediatamente após iniciar a instalação, pode ser informado de que não possui espaço livre suficiente no disco rígido para instalar o BitDefender. Nesse caso, liberte o espaço necessário em disco na partição onde quer que o BitDefender seja instalado e depois continue ou recomece a instalação.

- A instalação trava e possivelmente, o seu sistema bloqueia.Apenas o reiniciar restaura a responsividade do sistema.
- A instalação foi concluída, mas não pode utilizar algumas ou todas as funções BitDefender.

Para detectar o problema de uma falha na instalação e instalar o BitDefender, siga os seguintes passos:

1. **Limpe o sistema depois da falha de instalação.** Se a instalação falhar, algumas chaves de registo e ficheiros do BitDefender poderão manter-se no seu sistema. Podem também afectar o desempenho e a estabilidade do sistema. Por isso deve removê-los antes de tentar instalar o produto novamente.

   Se for este o caso, a solução mais fácil é remover totalmente o BitDefender do sistema e, depois, reinstalá-lo.Para mais informação, por favor consulte o “*Como Posso Remover Totalmente o BitDefender?*” (p. 262).

2. **Verificar causas possíveis para a instalação ter falhado.** Antes de avançar para reinstalar o produto, verifique e remova possíveis condições que podem ter causado a falha da instalação:

   a. Verifique se tem qualquer outra solução de segurança instalada na medida em que possam interferir no funcionamento normal do BitDefender. Se for este o caso, recomendamos que remova todas as outras soluções de segurança e reinstale BitDefender.

   b. Também deve verificar se seu sistema está infectado.Faça uma das coisas seguintes:

      - Utilize o BitDefender Rescue CD para analisar seu computador e remover quaisquer ameaças existentes.Para mais informação, por favor consulte o “*CD de Emergência BitDefender*” (p. 244).
      - Abra a janela do Internet Explorer, vá a www.bitdefender.com e execute a análise online (clique no botão **Analise Agora**).

3. Volte a tentar instalar o BitDefender.É recomendado que descarregue e execute a ultima versão do ficheiro de instalação em www.bitdefender.com.

4. Se a instalação falhar, contacte a BitDefender para suporte, como descrito na secção “*Apoio*” (p. 253).

40.2. O meu sistema parece estar lento

Normalmente, após a instalação de um software de segurança, o sistema poderá abrandar ligeiramente, o que é, até um certo nível, normal.

Se notar um abrandamento significativo, este problema pode dever-se às seguintes razões:

- **O BitDefender não é o único programa de segurança instalada no sistema.**

Apesar de o BitDefender procurar e remover os programas de segurança encontrados durante a instalação, é recomendado que remova todos os outros programas antivírus utilizados antes de instalar o BitDefender.Para mais informação, por favor consulte o “*Como Posso Remover Outras Soluções de Segurança?*” (p. 260).

- **Não estão cumpridos os Requisitos Mínimos do Sistema para executar o BitDefender.**

  Se o seu computador não cumprir os Requisitos Mínimos do Sistema, ficará lento, especialmente se estiver a executar muitas aplicações ao mesmo tempo.Para mais informação, por favor consulte o “*Requisitos Minímos do Sistema*” (p. 2).

- **Há demasiadas chaves de registo inválidas no seu Registo do Windows.**

  A limpeza do Registo do Windows pode melhorar o desempenho do seu sistema.Para mais informação, por favor consulte o “*Limpar o Registo do Windows*” (p. 188).

- **As unidades do seu disco rígido estão demasiado fragmentadas.**

  A fragmentação dos ficheiros abranda o acesso aos ficheiros e diminui o desempenho do sistema.

  A Desfragmentação do Disco pode melhorar o desempenho do seu sistema.Para mais informação, por favor consulte o “*Desfragmentar Volumes de Discos Duros*” (p. 185).

- **As aplicações executadas no seu sistema estão a consumir demasiados recursos.**

  O Monitor de Desempenho BitDefender permite-lhe determinar o impacto das aplicações executadas no seu sistema através da utilização do CPU, da memória e do disco rígido.

  Deve conseguir identificar as aplicações que estão a fazer com que o sistema tenha um mau desempenho, e fechar ou monitorizá-las.Para mais informação, por favor consulte o “*Monitor de Desempenho*” (p. 191).

40.3. A Análise Não Inicia

Este tipo de problema pode ter duas causas principais:

- **Uma instalação anterior do BitDefender que não foi totalmente removida ou uma instalação do BitDefender mal sucedida**.

  Se for este o caso, a solução mais fácil é remover totalmente o BitDefender do sistema e, depois, reinstalá-lo.Para mais informação, por favor consulte o “*Como Posso Remover Totalmente o BitDefender?*” (p. 262).

- **O BitDefender não é a única solução de segurança instalada no seu sistema**.

Neste caso, siga os passos seguintes:

1. Remover a outra solução de segurança.Para mais informação, por favor consulte o *"Como Posso Remover Outras Soluções de Segurança?"* (p. 260).
2. Remover o BitDefender totalmente do sistema.
3. Reinstalar o BitDefender no sistema.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção *"Apoio"* (p. 253).

40.4. Já Não Consigo Utilizar uma Aplicação

Este problema ocorre quando está a tentar utilizar um programa que estava a funcionar normalmente antes de instalar o BitDefender.

Poderá encontrar uma das seguintes situações:

- Poderá receber uma mensagem do BitDefender a informar que o programa está a tentar modificar o sistema.
- Pode receber uma mensagem de erro do programa que está a tentar utilizar.

Este tipo de situação ocorre quando o módulo de Controlo Activo de Vírus classifica erradamente algumas aplicações como maliciosas.

O Controlo de Vírus Activo é um módulo do BitDefender que monitoriza constantemente as aplicações executadas no seu sistema e denuncia o comportamento potencialmente malicioso.Como este recurso é baseado num sistema heurístico, poderá haver casos em que as aplicações legítimas são denunciadas pelo Controlo Activo de Vírus.

Quando isto acontece, pode excluir a respectiva aplicação da monitorização do Controlo Activo de Vírus.

Para adicionar o programa à lista de exclusões, siga os seguintes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivírus > Escudo**.
3. Clique em **Configuração Avançada**.
4. Na nova janela, abra o separador **Exclusões**, clique no botão **Adicionar** e procure a localização do ficheiro .exe do programa (normalmente localizado na pasta `C:\Programa`).
5. Clique em **OK** para guardar as alterações e fechar a janela.
6. Feche a janela do BitDefender e confirme se o problema ainda persiste.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção *"Apoio"* (p. 253).

40.5. Não Consigo Ligar à Internet

Poderá verificar que um programa já não consegue ligar à Internet ou aceder aos serviços em rede após a instalação do BitDefender.

O assistente de Resolução de Problemas vai ajudar a identificar e resolver o problema com a ligação.Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Segurança** e clique em **Configurar a Firewall**, nas Tarefas Rápidas, no lado esquerdo da janela.Seleccione o separador **Definições** na nova janela que aparece e clique em **Resolução de Problemas**.

Modo Avançado
: Vá a **Firewall > Definições** e clique em **Resolução de Problemas**.

Siga o procedimento de três passos para iniciar a resolução de problemas.Pode navegar pelo assistente utilizando o botão **Seguinte**.Para sair do assistente, clique em **Cancelar**.

1. **Bem-vindo**

   Seleccione **Estou a tentar aceder à Internet e a operação falha**.

2. **Identificar o Problema**

   Clique em **Fechar a Aplicação** e **Explorar** para localizar o ficheiro .exe do programa (normalmente localizado em `C:\Programas`, p.ex. Firefox.exe).Prima **Adicionar**.

3. **Solução Recomendada**

   Seleccione **Sim, permitir acesso**.Clique em **Concluir** e verifique se o problema ainda persiste.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção “*Apoio*” (p. 253).

40.6. Não Consigo Usar Uma Impressora

Dependendo da rede a que está ligado, a firewall do BitDefender poderá bloquear a ligação entre o seu computador e a impressora de rede.

Neste caso, a melhor solução é configurar o BitDefender para permitir automaticamente as ligações de e para a respectiva impressora.

O assistente de Resolução de Problemas vai ajudar a identificar e resolver o problema com a ligação.Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio

Abra o separador **Segurança** e clique em **Configurar a Firewall**, nas Tarefas Rápidas, no lado esquerdo da janela.Seleccione o separador **Definições** na nova janela que aparece e clique em **Resolução de Problemas**.

Modo Avançado

Vá a **Firewall > Definições** e clique em **Resolução de Problemas**.

Siga o procedimento de três passos para iniciar a resolução de problemas.Pode navegar pelo assistente utilizando o botão **Seguinte**.Para sair do assistente, clique em **Cancelar**.

1. **Bem-vindo**

   Seleccione **Estou a tentar imprimir e a operação falha**.

2. **Identificar o Problema**

   Clique em **Escolher Impressora**.Seleccione a impressora da lista, por nome ou endereço IP.Se não conseguir encontrar o dispositivo na lista, introduza o manualmente o endereço de IP no campo de edição.Prima **Adicionar**.

3. **Solução Recomendada**

   Seleccione **Sim, permitir acesso**.Clique em **Concluir** e verifique se o problema ainda persiste.

Se o assistente de Resolução de Problemas indicar que o problema não é causado pela firewall do BitDefender no seu computador, procure outras possíveis causas, como as seguintes:

- A firewall no outro computador poderá bloquear a partilha de ficheiros e impressoras com o seu computador.
  - Se o Firewall do Windows está a ser utilizada, pode ser configurada para permitir a partilha de ficheiros e impressora da seguinte fomra: abra a janela das definições do Firewall do Windows, separador **Excepções** e seleccione a caixa de selecção **Partilha de Ficheiros e Impressoras**.
  - Se outro programa de firewall estiver a ser utilizado, por favor consulte a documentação e ficheiro de ajuda.
- Condições gerais que podem impedir a utilização ou conexão com a impressora compartilhada:
  - Poderá precisar de se ligar com uma conta de administrador do Windows para aceder à impressora compartilhada.
  - As permissões são definidas para a impressora compartilhada para permitir acesso a um computador específico e apenas utilizadores.Se está a compartilhar a sua impressora, verifique as permissões definidas para a impressora para saber se o utilizador do outro computador está autorizado a aceder à impressora. Se está a tentar ligar-se a uma impressora compartilhada, verifique com o

utilizador do outro computador se tem permissão para se conectar com a impressora.

- A impressora ligada ao seu computador ou ao outro computador não está a ser compartilhada.
- A impressora compartilhada não está adicionada ao computador.

Nota
Para aprender como gerir o compartilhamento de impressoras (compartilhar uma impressora, definir ou remover permissões para a impressora, conecta-se a uma rede de impressora ou a uma impressora partilhada), vá à Ajuda e Suporte do Windows (no menu Iniciar, clique em **Ajuda e Suporte**).

- O acesso a uma impressora em rede pode ser restringido a computadores ou apenas a utilizadores. Deverá verificar com o administrador da rede se tem ou não permissão para aceder à impressora.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção “*Apoio*” (p. 253).

40.7. Não Consigo Partilhar Ficheiros Com Outro Computador

Dependendo da rede a que está ligado, a firewall do BitDefender poderá bloquear a ligação entre o seu sistema e outro computador.Em resultado, deixará de poder partilhar ficheiros com o outro computador.Neste caso, a melhor solução é configurar o BitDefender para permitir automaticamente as ligações de e para o respectivo sistema.

O assistente de Resolução de Problemas vai ajudar a identificar e resolver o problema com a ligação.Para iniciar o assistente, abra o BitDefender e, consoante o interface de utilizador, proceda da seguinte forma:

Modo Intermédio
: Abra o separador **Segurança** e clique em **Configurar a Firewall**, nas Tarefas Rápidas, no lado esquerdo da janela.Seleccione o separador **Definições** na nova janela que aparece e clique em **Resolução de Problemas**.

Modo Avançado
: Vá a **Firewall > Definições** e clique em **Resolução de Problemas**.

Siga o procedimento de três passos para iniciar a resolução de problemas.Pode navegar pelo assistente utilizando o botão **Seguinte**.Para sair do assistente, clique em **Cancelar**.

1. **Bem-vindo**

   >Seleccione **Estou a tentar aceder a um computador da minha rede e a operação falha**.

2. **Identificar o Problema**

   Clique em **Escolher Computador**.Seleccione o computador da lista, por nome ou endereço IP.Se não conseguir encontrar o computador na lista, introduza o manualmente o endereço de IP no campo de edição.Prima **Adicionar**.

3. **Solução Recomendada**

   Seleccione **Sim, permitir acesso**.Clique em **Concluir** e verifique se o problema ainda persiste.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção “*Apoio*” (p. 253).

40.8. A minha Internet está lenta

Esta situação poderá surgir depois de instalar o BitDefender.Este problema poderá ser causado por erros na configuração da firewall do BitDefender.

Para resolver esta situação, siga os seguintes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Firewall > Definições**.
3. Desmarque a caixa **A firewall está activada** para desactivar temporariamente a firewall.
4. Verifique se consegue ligar à Internet com a firewall do BitDefender desactivada.

   - Se ainda não conseguir ligar à Internet, o problema poderá não ser causado pelo BitDefender. Deve contactar o seu Fornecedor de Serviço de Internet para confirmar se a ligação está operacional.

     Se receber a confirmação do seu Fornecedor de Serviços de Internet que a ligação está operacional e o problema persistir, contacte a BitDefender como indicado na secção “*Apoio*” (p. 253).

   - Se conseguir ligar à Internet depois de desactivar a firewall do BitDefender, siga os seguintes passos:

     a. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.

     b. Vá a **Firewall > Definições** e seleccione a caixa para activar a Firewall.

     c. Clique em **Definições Avançadas**, seleccione **Activar Partilha de Ligação à Internet** e desmarque **Bloquear Análises de Porta**.

     d. Abra o separador **Rede** na janela principal.

     e. Abra o menu pendente da coluna **Tipo de Rede** e seleccione **Casa/ Escritório**.

f. Vá à coluna **Genérico** e defina-a como **Sim**. Defina o **Modo Stealth** como **Remoto**.

g. Verifique se pode ligar à Internet.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção *“Apoio”* (p. 253).

40.9. Como Actualizar o BitDefender numa Ligação à Internet Lenta

Se tiver uma ligação à Internet lenta (por exemplo, ligação telefónica), poderão ocorrer erros durante o processo de actualização.

Para manter o seu sistema actualizado com as mais recentes assinaturas de malware BitDefender, siga os seguintes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Actualização > Definições**.
3. Em **Definições da Actualização Manual**, seleccione **Perguntar antes de transferir actualizações**.
4. Clique em **Aplicar** e abra o separador **Actualizar**.
5. Clique em **Actualizar Agora** e aparecerá uma nova janela.
6. Seleccione apenas **Actualizações das assinaturas** e clique em **Ok**.
7. O BitDefender vai transferir e instalar apenas as actualizações das assinaturas de malware.

40.10. O Meu Computador Não Está Ligado à Internet. Como Posso Actualizar o BitDefender?

Se o seu computador não estiver ligado à Internet, tem de transferir manualmente as actualizações para um computador com acesso à Internet e, depois, transferi-las para o seu computador com um dispositivo amovível, por exemplo, um USB.

Siga estes passos:

1. Num computador com acesso à Internet, abra o navegador da Internet e vá a:

   www.bitdefender.com/site/view/Desktop-Products-Updates.html
2. Na coluna **Actualização Manual**, clique na hiperligação que corresponde ao seu produto e à arquitectura do sistema.Se não sabe se a versão do seu Windows é de 32 ou 64 bits, consulte *“Estou a Utilizar uma Versão de 32 ou 64 Bit do Windows?”* (p. 261).
3. Guarde o ficheiro com o nome `weekly.exe` no sistema.

4. Mova o ficheiro transferido para um dispositivo amovível, tal como uma unidade USB, e depois para o seu computador.
5. Faça duplo clique no ficheiro e siga os passos do assistente.

40.11. Os serviços BitDefender não estão a responder

Este artigo ajuda-o a troubleshoot os erros de*Os Serviços BitDefender não estão a responder*.Pode encontrar esse erro da seguinte forma:

- O icon BitDefender na Barra de Notificação está a cinzenta e um pop-up informa que os serviços do BitDefender não estão a responder.
- A janela do BitDefender indica que os serviços do BitDefender não estão a responder.

O erro pode ter ocorrido devido a um dos seguintes factores:

- Está a ser instalada uma actualização importante.
- problemas temporários de comunicação entre os serviços da BitDefender.
- alguns dos serviços da BitDefender estão parados.
- Outras soluções de segurança em execução no seu computador, ao mesmo tempo que o BitDefender.
- Os vírus no seu sistema afectam o funcionamento normal do BitDefender.

Para solucionar este erro, tente estas soluções:

1. Espere uns momentos e verifique se existe alguma alteração.Este erro pode ser temporário.
2. Reinicie o computador e aguarde alguns momentos até o BitDefender iniciar. Abra o BitDefender e veja se o erro se mantém.Reiniciar o computador normalmente resolve o problema.
3. Verifique se tem qualquer outra solução de segurança instalada na medida em que possam interferir no funcionamento normal do BitDefender. Se for este o caso, recomendamos que remova todas as outras soluções de segurança e reinstale BitDefender.
4. Se o erro persistir, pode haver um problema mais grave (por exemplo, pode estar infectado com um vírus que interfere com o BitDefender).Por favor contacte a BitDefender para suporte, como descrito na secção “*Apoio*” (p. 253).

40.12. O Filtro Antispam Não Está a Funcionar Correctamente

Este artigo ajuda a solucionar os seguintes problemas relacionados com a operação de filtragem do Antispam do BitDefender:

- Um número de mensagens de e-mail legítimas são marcadas como `[spam]`.

- Muitas mensagens spam não estão marcadas de acordo com o filtro antispam.
- O filtro antispam não detecta qualquer mensagem de spam.

40.12.1. Mensagens Legítimas são marcadas como [spam]

Mensagens legítimas são marcadas como `[spam]` simplesmente porque elas parecem spam para o filtro antispam do BitDefender.Pode normalmente resolver este problema ao configurar adequadamente o filtro Antispam.

O BitDefender adiciona automaticamente os remetentes das suas mensagens de e-mail à Lista de Amigos.As mensagens de e-mail recebidas dos contactos na lista de Amigos são consideradas legítimas. Elas não são verificadas pelo filtro antispam e, deste modo, elas nunca são marcadas como `[spam]`.

A configuração automática da lista de Amigos não impede a detecção de erros que podem ocorrer nestas situações:

- Recebeu muitos e-mails publicitários solicitados como resultado de se inscrever em vários sites.Neste caso, a solução é adicionar à Lista de Amigos o endereço de e-mail do qual recebeu esses e-mails.
- Uma parte significativa dos seus mails legitimos são de pessoas com quem nunca trocou e-mails antes, tais como clientes, potenciais parceiros empresariais e outros.Outras soluções são requeridas neste caso.

Se estiver a utilizar um cliente de e-mail com o qual o BitDefender é compatível, experimente uma das seguintes soluções:

1. Indica detecção de erros. Isto é utilizado para treinar o Motor de Aprendizagem (Bayesiano) do filtro de antispam e ajuda a prevenir futuros erros de detecção.O Motor de Aprendizagem analisa as mensagens indicadas e aprende os seus padrões. Os próximos e-mails que se encaixem nos mesmos padrões, não serão marcadas como `[spam]`.
2. Diminui o nível de protecção antispam. Ao diminuir o nível de protecção, o filtro de antispam necessitará de mais indicadores de spam para classificar uma mensagem de e-mail como spam.Experimente esta solução apenas se várias mensagens legitimas (incluindo mensagens publicitárias solicitadas) estão a ser incorrectamente detectadas como spam.
3. Retreinar o Motor de Aprendizagem (filtro Bayesiano). Tente esta solução unicamente se as soluções anteriores não oferecem resultados satisfatórios.

Nota

O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns.Para ver a lista completa de clientes de e-mail suportados, por favor consulte o “*Requisitos de Software*” (p. 2).

Se está a utilizar um mail de cliente diferente, não pode indicar detecção de erros e instruir o Motor de Aprendizagem. Para resolver este problema, tente diminuir o nível de protecção antispam.

Adicionar os Contactos à Lista de Amigos

Se está a utilizar um cliente de mail suportado, pode facilmente adicionar os remetentes das mensagens legítimas à lista de Amigos.Siga estes passos:

1. No seu cliente de mail, seleccione a mensagem de e-mail do remetente que quer adicionar à lista de Amigos.
2. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do BitDefender.
3. Poderá ser convidado a reconhecer os endereços adicionados à lista de Amigos.Seleccione **Não mostrar esta mensagem outra vez** e clique **OK**.

Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.

Se está a utilizar um cliente de mail diferente, poderá adicionar os contactos à lista Amigos a partir do interface do BitDefender.Siga estes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Clique em **Antispam** do lado esquerdo do menu.
3. Clique na barra **Estado**.
4. Clique em **Gerir Amigos**.A janela de configuração irá aparecer.
5. Digite o endereço de e-mail de que quer receber sempre mensagens e cique no botão para adicionar o endereço à Lista de Amigos.
6. Clique em **OK** para guardar as alterações e fechar a janela.

Indique os Erros de Detecção.

Se estiver a usar um cliente de e-mail suportado, pode facilmente corrigir o filtro antispam (indicando mensagens de correio electrónico que não deveriam ter sido marcadas como`[spam]`). Se o fizer, irá melhorar consideravelmente a eficiência do filtro antispam.Siga estes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo electrónico, para onde são movidas as mensagens.
3. Seleccione a mensagem legítima incorrectamente marcada como `[spam]` pelo BitDefender.
4. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do BitDefender para adicionar o remetente à lista de Amigos.Pode necessitar de

clicar em **OK** para confirmar.Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.

5. Clique no botão **Não é Spam** na barra de antispam BitDefender (normalmente localizada na parte superior da janela do cliente de e-mail). Isto indica ao Mecanismo de Aprendizagem que a mensagem seleccionada não é spam. A mensagem de e-mail será movida para a pasta Recebidos.Os próximos e-mails que se encaixem nos mesmos padrões, não serão marcadas como `[spam]`.

Diminuir o Nível de Protecção do Antispam

Para diminuir o nível de protecção do antispam, siga estes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Clique em **Antispam** do lado esquerdo do menu.
3. Clique na barra **Estado**.
4. Baixe a seta na barra deslocação.

É recomendado a baixar apenas um nível de protecção e depois espere o tempo suficiente para avaliar os resultados.Se muitas mensagens de e-mail legitimas continuam a ser marcadas como `[spam]`, pode baixar o nível de protecção. Se reparar que muitas mensagens spam nao estão a ser detectadas, não deverá baixar o nível de protecção.

Retreinar o Motor de Aprendizagem (Bayesiano)

Antes de iniciar o treino do Motor de Aprendizagem (Bayesiano), prepare uma pasta que contenha apenas mensagens SPAM e outra que contenha apenas mensagens legitimas.O Motor de Aprendizagem irá analisá-los e aprender as características que o definem como spam ou legitimar mensagens que normalmente recebe. Para que a formação seja eficaz, tem de haver mais de 50 mensagens em cada categoria.

Para redefinir a base de dados Bayesiana e retreinar o Motor de Aprendizagem, siga os seguintes passos:

1. Abra o mail de cliente.
2. Na barra de ferramentas antispam do BitDefender, clique no botão **Assistente** para iniciar o assistente de configuração do antispam.
3. Clique **Seguinte**.
4. Seleccione **Saltar este passo** e clique em **Seguinte**.
5. Seleccione **Limpar dados do filtro antispam** e clique **Seguinte**.
6. Seleccione a pasta que contém as mensagens legítimas e clique em **Seguinte**.
7. Seleccione a pasta que contém as mensagens SPAM e clique em **Seguinte**.

8. Clique em **Terminar** para dar início ao processo de treino.
9. Quando o treino está completo, clique em **Fechar**.

Pedir Ajuda

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção “*Apoio*” (p. 253).

40.12.2. Muitas Mensagens de Spam Não São Detectadas

Se está a receber muitas mensagens spam que não estão marcadas como `[spam]`, tem de configurar o filtro antispam BitDefender de modo a melhorar a sua eficiência.

Se estiver a utilizar um cliente de e-mail com o qual o BitDefender é compatível, experimente uma das seguintes soluções:

1. Indica mensagens de spam não detectadas. Isto é utilizado para treinar o Motor de Aprendizagem (Bayesiano) do filtro de antispam e ajuda a melhorar a detecção do antispam.O Motor de Aprendizagem analisa as mensagens indicadas e aprende os seus padrões. Os próximos e-mails que se encaixem nos mesmos padrões, serão marcadas como `[spam]`.
2. Adicione spammers à lista de Spammers. As mensagens de e-mail recebidas dos endereços na lista de Spammers são automaticamente marcadas como `[spam]`.
3. Aumente o nível de protecção antispam. Ao aumentar o nível de protecção, o filtro de antispam necessitará de menos indicadores de spam para classificar uma mensagem de e-mail como spam.
4. Retreinar o Motor de Aprendizagem (filtro Bayesiano). Utilize esta solução quando a detecção antispam for muito insatisfatória e a indicação de mensagens de spam não detectadas, não funcionar mais.

Nota

O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns.Para ver a lista completa de clientes de e-mail suportados, por favor consulte o “*Requisitos de Software*” (p. 2).

Se está a utilizar um mail de cliente diferente, não pode mais indicar mensagens spam e instruir o Motor de Aprendizagem. Para resolver este problema, tente aumentar o nível de protecção e adicionar spams à lista Spammers.

Indica Mensagens de Spam não detectadas

Se estiver a utilizar um cliente de e-mail suportado, pode facilmente indicar quais as mensagens de e-mail que devem ser detectadas como spam. Ao fazê-lo melhora, em muito, a eficiência do filtro de antispam.Siga estes passos:

1. Abra o mail de cliente.

2. Vá à pasta Caixa de Entrada.
3. Seleccione as mensagens spam não detectadas
4. Clique no botão **É Spam** na barra de tarefas do BitDefender (normalmente localizada na parte superior da janela de cliente de mail). Isto indica ao Motor de Aprendizagem que as mensagens seleccionadas são spam. São imediatamente marcadas como `[spam]` e movidas para a pasta de lixo electrónico.Os próximos e-mails que se encaixem nos mesmos padrões, serão marcadas como `[spam]`.

Adicionar Spammers à lista de Spammers

Se está a utilizar um cliente de mail suportado, pode facilmente adicionar os remetentes das mensagens spam à lista Spammers.Siga estes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo electrónico, para onde são movidas as mensagens.
3. Seleccione a mensagem marcada como `[spam]` pela BitDefender.
4. Clique no botão **Adicionar Spammer** da barra de tarefas antispam do BitDefender.
5. Poderá ser convidado a reconhecer os endereços como Spammers.Seleccione **Não mostrar esta mensagem outra vez** e clique **OK**.

Se está a ultizar uma conta de mail diferente, pode manualmente adicionar spammers à lista Spammers do interface do BitDefender. É conveniente que o faça apenas quando receber várias mensagens spam do mesmo endereço e-mail.Siga estes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Clique em **Antispam** do lado esquerdo do menu.
3. Clique na barra **Estado**.
4. Clique em **Gerir Spammers**.A janela de configuração irá aparecer.
5. Digite o email do spam e clique no botão para adicionar o endereço à Lista Spammers.
6. Clique em **OK** para guardar as alterações e fechar a janela.

Aumentar o Nível de Protecção do Antispam

Para aumentar o nível de protecção do antispam, siga estes passos:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Clique em **Antispam** do lado esquerdo do menu.

3. Clique na barra **Estado**.
4. Suba a seta na barra deslocação.

Retreinar o Motor de Aprendizagem (Bayesiano)

Antes de iniciar o treino do Motor de Aprendizagem (Bayesiano), prepare uma pasta que contenha apenas mensagens SPAM e outra que contenha apenas mensagens legitimas.O Motor de Aprendizagem irá analisá-los e aprender as características que o definem como spam ou legitimar mensagens que normalmente recebe. Para que a formação seja eficaz, tem de haver mais de 50 mensagens em cada pasta.

Para redefinir a base de dados Bayesiana e retreinar o Motor de Aprendizagem, siga os seguintes passos:

1. Abra o mail de cliente.
2. Na barra de ferramentas antispam do BitDefender, clique no botão **Assistente** para iniciar o assistente de configuração do antispam.
3. Clique **Seguinte**.
4. Seleccione **Saltar este passo** e clique em **Seguinte**.
5. Seleccione **Limpar dados do filtro antispam** e clique **Seguinte**.
6. Seleccione a pasta que contém as mensagens legítimas e clique em **Seguinte**.
7. Seleccione a pasta que contém as mensagens SPAM e clique em **Seguinte**.
8. Clique em **Terminar** para dar início ao processo de treino.
9. Quando o treino está completo, clique em **Fechar**.

Pedir Ajuda

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção “*Apoio*” (p. 253).

40.12.3. O Filtro Antispam Não Detecta Nenhuma Mensagem Spam

Se nenhuma mensagem spam for marcada como `[spam]`, poderá haver algum problema como o filtro Antispam do BitDefender.Antes de resolver este problema, certifique-se de que não é causado por nenhuma das seguintes condições:

- A protecção de Antispam do BitDefender está disponível apenas para clientes de correio electrónico configurado para receber mensagens de e-mail via protocolo POP3.Isto significa o seguinte:
  - As mensagens de Email obtidas atraves de Webmail (Yahoo, Gmail, Hotmail ou outros) não são filtradas como spam pelo BitDefender.

▶ Se o seu cliente de e-mail está configurado para receber mensagens de e-mail usando outro protocolo que não o POP3 (por exemplo, IMAP4), o filtro Antispam do BitDefender não as analisará à procura de spam.

Nota

POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio.Se você não sabe o protocolo que o seu cliente de e-mail utiliza para importar mensagens de e-mail, solicite à pessoa que o configurou.

- O BitDefender Total Security 2011 não analisa o tráfego POP3 do Lotus Notes.

Deverá também verificar as possiveis seguintes causas:

1. Certifique-se que o Antispam está activado.
   a. Abrir o BitDefender.
   b. Clique no botão **Opções** no canto superior direito da janela e seleccione **Preferências**.
   c. Nas Definições de Segurança, verifique o estado do antispam.

   Se o Antispam estava desactivado, era isso que estava a causar o problema.Active o Antispam e acompanhe a operação para ver se o problema é corrigido.
2. Embora seja muito improvável, poderá ver se você (ou alguém) configurou o BitDefender para não marcar as mensagens spam como `[spam]`.
   a. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
   b. Clique em **Antispam** localizado no lado esquerdo do menu e em seguida clique no separador **Definições**.
   c. Assegure-se de que a opção **Marcar mensagens spam como spam no assunto** está seleccionada.

Uma solução possível é reparar ou reinstalar o produto. Contudo, poderá contactar a BitDefender para suporte, como descrito na secção “*Apoio*” (p. 253).

40.13. A Desinstalação do BitDefender Falhou

Este artigo ajuda-o a resolver erros que possam ocorrer quando remover o BitDefender.Há duas situações possíveis:

- Durante a remoção, aparece uma imagem de erro.O ecrã apresenta um botão para executar uma ferramenta de desinstalação que irá limpar o sistema.
- A remoção trava e possivelmente, o seu sistema bloqueia.Clique em **Cancelar** para abortar a desinstalação. Se isso não funcionar, reinicie o sistema.

Se a desinstalação falhar, algumas chaves de registo e ficheiros do BitDefender poderão manter-se no seu sistema. Esses resquícios podem impedir uma nova instalação do BitDefender. Podem também afectar o desempenho e a estabilidade

do sistema.Para remover completamente o BitDefender do seu sistema, deverá executar a ferramenta de desinstalação.

Para mais informação, por favor consulte o “*Como Posso Remover Totalmente o BitDefender?*” (p. 262).

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção “*Apoio*” (p. 253).

41. Remover Malware do Sistema

O malware pode afectar o seu sistema de várias formas e a actuação do BitDefender depende do tipo de ataque por malware.Como os vírus alteram frequentemente o modo de acção, é difícil estabelecer um padrão com base no comportamento e nas acções.

Há situações em que o BitDefender não consegue remover automaticamente a infecção por malware do seu sistema.Nestes casos, a sua intervenção é necessária.

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da BitDefender como mostrado no capítulo “*Apoio*” (p. 253).

41.1. CD de Emergência BitDefender

CD de Recuperação do BitDefender é um recurso incluído na maioria dos CDs de instalação do BitDefender que permite analisar e desinfectar todos os discos rígidos existentes antes de o seu sistema operativo arrancar.Também pode ajudar a guardar dados do seu computador Windows em risco num dispositivo amovível.

Se não possuir um CD de Recuperação do BitDefender, pode transferir na forma de imagem ISO a partir do seguinte local:

http://download.bitdefender.com/rescue_cd/

Transfira o ficheiro .iso e grave-o num CD ou DVD com uma ferramenta à sua escolha.

Analisar o Sistema com o CD de Recuperação do BitDefender

Para analisar o seu sistema com o CD de Recuperação do BitDefender, siga os seguintes passos:

1. Configure a BIOS do seu computador para desligar o CD.
2. Coloque o CD na unidade e reinicie o computador.
3. Aguarde que o ecrã do BitDefender apareça e seleccione **Iniciar CD de Recuperação do BitDefender** no idioma preferido.
4. Aguarde que o processo de arranque termine. Poderá demorar algum tempo.
5. Assim que estiver concluído o processo de arranque, as assinaturas do BitDefender são automaticamente actualizadas e é iniciada uma análise a todas as partições do disco rígido detectadas.

Guardar Dados com o CD de Recuperação do BitDefender

vamos partir do principio que não consegue arrancar o seu PC em Windows PC devido a incidências desconhecidas. Ao mesmo tempo, você necessita desesperadamente de aceder a alguma informação importante do seu computador.

Eis aqui uma situação em que o CD de Emergência BitDefender se revela extremamente útil.

Para guardar os seus dados do computador para um dispositivo amovível, tal como um dispositivo USB, siga os seguintes passos:

1. Configure a BIOS do seu computador para desligar o CD.
2. Coloque o CD na unidade e reinicie o computador.
3. Aguarde que o ecrã do BitDefender apareça e seleccione **Iniciar CD de Recuperação do BitDefender** no idioma preferido.
4. Aguarde que o processo de arranque termine. Poderá demorar algum tempo.
5. Assim que estiver concluído o processo de arranque, as assinaturas do BitDefender são automaticamente actualizadas e é iniciada uma análise a todas as partições do disco rígido detectadas.

   As partições do seu disco rígido irão aparecer no ambiente de trabalho. Para ver o conteúdo de um disco numa janela semelhante ao Explorador do Windows, faça duplo-clique.

   Nota

   Ao trabalhar com o CD de Recuperação do BitDefender, estará a trabalhar com nomes de partição do tipo Linux. Os discos que não forem etiquetados no Windows aparecerão como `[LocalDisk-0]`, correspondendo, provavelmente, à `(C:)` partição de tipo Windows, `[LocalDisk-1]` correspondendo a `(D:)` e assim sucessivamente.

6. Ligue o dispositivo amovível a uma porta USB do seu computador.Brevemente aparecerá uma janela a mostrar o conteúdo do dispositivo.
7. Pode copiar ficheiros e pastas normalmente, tal como no ambiente do Windows.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção “*Apoio*” (p. 253).

41.2. O Que Fazer Se o BitDefender Encontrar Vírus No Seu Computador?

Pode verificar se há um vírus no seu computador de uma das seguintes formas:

- O BitDefender analisou o seu computador e encontrou itens infectados.
- Um alerta de vírus avisa que o BitDefender bloqueou um ou vários vírus no seu computador.

Nestas situações, actualize o BitDefender para se certificar que tem as assinaturas de malware mais recentes e realize uma Análise Minuciosa ao Sistema.

Assim que a análise minuciosa terminar, seleccione a acção pretendida para os itens infectados (Desinfectar, Eliminar, Mover para a Quarentena).

Atenção

Se suspeitar que o ficheiro faz parte do sistema operativo do Windows ou que não é um ficheiro infectado, não siga estes passos e contacte e Apoio ao Cliente do BitDefender assim que possível.

Se não for possível efectuar a acção seleccionada e o relatório da análise indicar uma infecção que não foi possível eliminar, tem de remover o(s) ficheiro(s) manualmente:

O primeiro método pode ser utilizado no modo Normal:

1. Desactive a protecção antivírus em tempo real do BitDefender.Para saber como fazer isto, consulte "*Como Posso Activar/Desactivar a Protecção Em Tempo Real*" (p. 262).
2. Mostrar objectos ocultos no Windows.Para saber como fazer isto, consulte "*Como Posso Mostrar Objectos Ocultos no Windows?*" (p. 263).
3. Procure a localização do ficheiro infectado (veja no relatório da análise) e elimine-o.
4. Active a protecção antivírus em tempo real do BitDefender.

No caso de o primeiro método falhar ao remover a infecção, siga os seguintes passos:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança.Para saber como fazer isto, consulte "*Como Posso Reiniciar no Modo de Segurança?*" (p. 261).
2. Mostrar objectos ocultos no Windows.
3. Procure a localização do ficheiro infectado (veja no relatório da análise) e elimine-o.
4. Reinicie o seu sistema e inicie sessão no modo normal.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção "*Apoio*" (p. 253).

41.3. Como Posso Limpar o Vírus de um Arquivo?

Um arquivo é um ficheiro ou um conjunto de ficheiros comprimidos num formato especial para reduzir o espaço no disco necessário para armazenar os ficheiros.

Alguns destes formatos são formatos livres, possibilitando ao BitDefender a opção de analisar o conteúdo e aplicar as acções adequadas para os remover.

Outros formatos de arquivo estão parcial ou totalmente fechados, mas o BitDefender só pode detectar a presença de vírus no interior, mas não pode aplicar outras acções.

Se o BitDefender avisar que foi detectado um vírus dentro de um arquivo e não estiver disponível uma acção, significa que não é possível remover o vírus devido a restrições nas definições de permissão do arquivo.

Pode limpar um vírus armazenado num arquivo da seguinte forma:

1. Identifique o arquivo que contém o vírus realizando uma Análise Minuciosa ao Sistema.
2. Desactive a protecção antivírus em tempo real do BitDefender.
3. Vá à localização do arquivo e descomprima-o com uma aplicação de arquivo, como o WinZip.
4. Identifique e elimine o ficheiro infectado.
5. Elimine o arquivo original de modo a garantir que a infecção é totalmente removida.
6. Comprima novamente os ficheiros num novo arquivo com uma aplicação de arquivo, como o WinZip.
7. Active a protecção antivírus em tempo real do BitDefender e execute uma análise minuciosa ao sistema para se certificar que não há outras infecções no sistema.

Nota
É importante saber que um vírus armazenado num arquivo não é uma ameaça imediata ao seu sistema pois o vírus tem de ser descomprimido e executado de modo a infectar o seu sistema.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção "*Apoio*" (p. 253).

41.4. Como Posso Limpar o Vírus de um Arquivo de Correio Electrónico?

O BitDefender também pode identificar vírus em bases de dados de correio electrónico e arquivos de correio electrónico armazenados no disco.

Por vezes, é necessário identificar a mensagem infectada com a informação fornecida no relatório da análise, e elimine-o manualmente.

Pode limpar um vírus armazenado num arquivo de correio electrónico da seguinte forma:

1. Analisar a base de dados do correio electrónico com o BitDefender.
2. Desactive a protecção antivírus em tempo real do BitDefender.
3. Abra o relatório da análise e utilize a informação de identificação (Assunto, De, Para) das mensagens infectadas para localizá-las no cliente de correio electrónico.

4. Elimine as mensagens infectadas.A maioria dos clientes de correio electrónico move a mensagem eliminada para uma pasta de recuperação, a partir da qual pode ser recuperada.Deve certificar-se que a mensagem também é eliminada desta pasta de recuperação.
5. Compactar a pasta com a mensagem infectada.
   - No Outlook Express:No menu Ficheiro, clique em Pasta e, depois em Compactar Todas as Pastas.
   - No Microsoft Outlook:No menu Ficheiro, clique em Gestão de Ficheiros de Dados.Seleccione os ficheiros das pastas (.pst) que pretende compactar e clique em Definições.Clique em Compactar.
6. Active a protecção antivírus em tempo real do BitDefender.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção “*Apoio*” (p. 253).

41.5. Como Posso Analisar o Computador no Modo de Segurança?

A análise manual BitDefender deixa-o analisar uma determinada pasta ou partição do disco sem ter de criar uma tarefa de análise.

Esta ferramenta foi desenhada para ser usada quando o Windows está a correr em Modo de Segurança.

Se o seu sistema está infectado com um vírus que não pode ser removido no modo normal, pode tentar remover o vírus iniciando o Windows em Modo de Segurança e analisando cada partição do disco rígido usando a Análise Manual BitDefender.

Para saber como pode aceder ao Modo de Segurança, consulte “*Como Posso Reiniciar no Modo de Segurança?*” (p. 261).

1. Para analisar o seu computador com a Análise Manual do BitDefender, siga o seguinte caminho a partir do menu Iniciar do Windows: **Iniciar** → **Todos os Programaas** → **BitDefender 2011** → **Análise Manual BitDefender**.
2. Clique em **Adicionar Pasta** para seleccionar o alvo da análise. Aparecerá uma nova janela.
3. Seleccione o alvo da análise :
   - para analisar o seu ambiente de trabalho, seleccione apenas **Ambiente de Trabalho**.
   - para analisar a partição do disco rígido completa, seleccione-a no **Meu Computador**.
   - para analisar uma determinada pasta, localize-a e seleccione-a.
4. Clique em **Ok** e **Continuar** para iniciar a análise.

5. Siga o assistente de Análise Antivírus para completar a análise.

41.6. O Que Fazer Se o BitDefender Identificou um Ficheiro Limpo como Infectado?

Há situações em que o BitDefender assinala erradamente um ficheiro legítimo como sendo uma ameaça (um falso positivo).Para corrigir este erro, adicione o ficheiro à área de Exclusões do BitDefender:

1. Desactive a protecção antivírus em tempo real do BitDefender.Para saber como fazer isto, consulte *"Como Posso Activar/Desactivar a Protecção Em Tempo Real"* (p. 262).
2. Mostrar objectos ocultos no Windows.Para saber como fazer isto, consulte *"Como Posso Mostrar Objectos Ocultos no Windows?"* (p. 263).
3. Restaurar o ficheiro da área de Quarentena.
4. Insira o ficheiro na área de Exclusões.
5. Active a protecção antivírus em tempo real do BitDefender.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção *"Apoio"* (p. 253).

41.7. Como Limpar os Ficheiros Infectados da Informação de Volume de Sistema

A pasta de Informação de Volume do Sistema é uma zona no seu disco rígido criada pelo Sistema Operativo e utilizada pelo Windows para armazenar informações essenciais relacionadas com a configuração do sistema.

Os motores do BitDefender podem detectar qualquer ficheiro infectado armazenado na Informação de Volume de Sistema mas, sendo esta uma área protegida, poderá não conseguir removê-lo.

Os ficheiros infectados detectados nas pastas do Restauro do Sistema aparecerão no relatório da análise da seguinte forma:

```
?:\Informação de Volume de Sistema\_restore{B36120B2-BA0A-4E5D-…
```

Para remover total e imediatamente o(s) ficheiro(s) infectado(s) do armazém de dados, desactive e reactive o recurso do Restauro do Sistema.

Se o Restauro do Sistema estiver desactivado, todos os pontos de restauro são removidos.

Quando o Restauro do Sistema é novamente activado, são criados novos pontos de restauro consoante as necessidades do agendamento e de eventos.

Para desactivar o Restauro do Sistema, siga os seguintes passos:

- **Para o Windows XP:**
  1. Siga este caminho: **Iniciar → Todos os Programas → Acessórios → Ferramentas do Sistema → Restauro do Sistema**
  2. Clique em **Definições do Restauro do Sistema**, na lado esquerdo da janela.
  3. Seleccione a caixa **Desactivar o Restauro do Sistema** em todas as unidades e clique em **Aplicar**.
  4. Quando receber a notificação que todos os Pontos de Restauro serão eliminados, clique em **Sim** para continuar.
  5. Para activar o Restauro do Sistema, desmarque a caixa **Desactivar o Restauro do Sistema** em todas as unidades e clique em **Aplicar**.
- **Para o Windows Vista:**
  1. Siga o seguinte caminho: **Iniciar → Painel de Controlo → Sistema e Manutenção → Sistema**
  2. No painel da esquerda, clique em **Protecção do Sistema**.

     Se lhe for pedida a palavra-passe de administrador ou a confirmação, escreva a palavra-passe ou dê a confirmação.
  3. Para desactivar a Restauração do Sistema, desmarque as caixas de selecção de cada unidade e clique em **Ok**.
  4. Para activar o Restauro do Sistema, desmarque as caixas de selecção de cada unidade e clique em **Ok**.
- **Para o Windows 7:**
  1. Clique em **Iniciar**, clique com o botão direito em **Computador** e clique em **Propriedades**.
  2. Clique na hiperligação da **Protecção do sistema** no painel da esquerda.
  3. Nas opções da **Protecção do Sistema**, seleccione a letra de cada unidade e clique em **Configurar**.
  4. Seleccione **Desactivar protecção do sistema** e clique em **Aplicar**.
  5. Clique em **Eliminar**, clique em **Continuar** quando pedido e, depois, clique em **Ok**.

Se esta informação não o ajudou, poderá contactar a BitDefender para suporte, como descrito na seccção “*Apoio*” (p. 253).

41.8. O que são Ficheiros Protegidos por Palavra-Passe no Relatório de Análise?

Isto é apenas uma notificação que indica que o BitDefender detectou que estes ficheiros estão protegidos por palavra-passe ou por outra forma de encriptação.

Normalmente, os itens protegidos por palavra-passe são:

- Ficheiros que pertencem a outras solução de segurança.
- Ficheiros que pertencem ao sistema operativo.

Para analisar verdadeiramente os conteúdos, estes ficheiros têm de ser extraídos ou de outra forma descodificados.

Se estes conteúdos pudessem ser extraídos, o verificador em tempo real do BitDefender analisaria-os automaticamente para manter o seu computador protegido.Se pretende analisar esses ficheiros com BitDefender, terá de contactar o fabricante do produto para receber mais informações sobre esses ficheiros.

Recomendamos que ignore estes ficheiros pois não constituem uma ameaça ao seu sistema.

41.9. O Que São os Itens Ignorados no Relatório de Análise?

Todos os ficheiros que aparecem como Ignorados no relatório de análise estão limpos.

Para um melhor desempenho, o BitDefender não analisa ficheiros que não tenham sido alterados desde a última análise.

41.10. O que são os Ficheiros Sobre-Comprimidos no Relatório de Análise?

Os itens sobre-comprimidos são elementos que não puderam ser extraídos pelo motor de análise ou elementos para os quais a desencriptação levaria demasiado tempo, tornando o sistema instável.

Sobre-comprimido significa que o BitDefender não realizou a análise a esse arquivo pois a descompactação iria consumir demasiados recursos do sistema. O conteúdo será analisado aquando o acesso em tempo real, se necessário.

41.11. Porque é que o BitDefender eliminou automaticamente um ficheiro infectado?

Se for detectado um ficheiro infectado, o BitDefender tentará automaticamente desinfectá-lo.Se a desinfecção falhar, o ficheiro é movido para a quarentena de modo a restringir a infecção.

Para determinados tipos de malware, a desinfecção não é possível por o ficheiro detectado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

Este é, normalmente, o caso de ficheiros de instalação que são transferidos de sítios de Internet suspeitos.Se se encontrar numa situação assim, transfira o ficheiro de instalação do sítio de Internet do fabricante ou de outro sítio fiável.

42. Apoio

A BitDefender esforça-se por fornecer aos seus clientes um nível de suporte rápido e eficaz.Se encontrar algum problema ou se tiver alguma questão sobre o nosso produto BitDefender, pode utilizar vários recursos em linha para encontrar rapidamente uma solução ou resposta.Ou, se preferir, pode contactar a equipa de Apoio ao Cliente da BitDefender. Os nossos técnicos de apoio responderão atempadamente às suas questões e dar-lhe-ão a ajuda que precisar.

42.1. Recursos Em Linha

Estão disponíveis vários recursos em linha para o ajudar a resolver problemas e a responder a questões relacionados com o BitDefender.

- Base de Conhecimento do BitDefender:http://www.bitdefender.com/help
- Fórum de Suporte BitDefender:http://forum.bitdefender.com
- o portal de segurança informática Malware City:http://www.malwarecity.com
- os Tutoriais

Também pode utilizar o seu motor de busca favorito para saber mais sobre a segurança de computadores, os produtos BitDefender e a empresa.

42.1.1. Base de Conhecimento do BitDefender

A BitDefender Knowledge Base é um repositório de informação on-line acerca dos produtos BitDefender. Armazena, num formato de relatório facilmente acessível, os resultados das actividades de reparação de erros por parte da equipe técnica do suporte BitDefender e da equipe de desenvolvimento, isto juntamente com artigos gerais acerca de prevenção de vírus, a administração de soluções BitDefender e explicações pormenorizadas, e muitos outros artigos.

A BitDefender Knowledge Base encontra-se aberta ao público e pode ser utilizada gratuitamente. Esta abundância de informação é uma outra forma de dar aos clientes BitDefender o conhecimento e o aprofundamento que eles necessitam. Todos os pedidos de informação ou relatórios de erro válidos originários de clientes BitDefender são incluídos na BitDefender Knowledge Base, como relatórios de reparação de erros, ou artigos informativos como suplementos aos ficheiros de ajuda dos produtos.

A BitDefender Knowledge Base encontra-se disponível a qualquer altura em http://kb.bitdefender.com.

42.1.2. Fórum de Suporte BitDefender

O Fórum de Suporte do BitDefender proporciona aos utilizadores do BitDefender uma forma fácil de obter ajuda e ajudar os outros.

Se o seu produto BitDefender não estiver a funcionar correctamente, se não conseguir remover certos vírus do seu computador ou se tiver alguma questão sobre a forma como opera, coloque o seu problema ou a sua questão no fórum.

Os técnicos de apoio da BitDefender supervisionam o fórum, à espera de novas mensagens para fornecer ajuda. Também pode receber uma resposta ou solução de um utilizador mais experiente do BitDefender.

Antes de publicar o seu problema ou questão, por favor pesquise o fórum por um tópico semelhante ou relacionado.

O Fórum de Suporte do BitDefender está disponível em http://forum.bitdefender.com, em 5 idiomas diferentes: inglês, alemão, francês, espanhol e romeno.Clique na hiperligação **Protecção Casa & Casa/Escritório** para aceder à secção dedicada aos produtos de consumidor.

42.1.3. Portal Malware City

O portal Malware City é uma excelente fonte de informações relacionadas com segurança informática. Aqui, pode ficar a conhecer as várias ameaças a que o seu computador fica exposto quando ligado à Internet (malware, phishing, spam, cibercriminosos).Um dicionário útil que ajuda a compreender os termos de segurança informática que não conhece.

Os novos artigos são publicados regularmente para o manter actualizado sobre as últimas ameaças descobertas, as actuais tendências de segurança e outras informações sobre a indústria de segurança informática.

A página de Internet do Malware City é http://www.malwarecity.com.

42.1.4. Tutoriais

Os tutoriais vão orientá-lo passo-a-passo na configuração do produto.São criadas de forma simples e directa para passar a mensagem.

O objectivo mais importante é garantir uma experiência agradável providenciando informações básicas e intermédias sobre os princípios de segurança, como configurar e utilizar o BitDefender.

O objectivo principal é eliminar a necessidade de obter ajuda especializada com os tutoriais que fornecem informações específicas sobre como utilizar e configurar o BitDefender.

Por exemplo, em vez de telefonar ao apoio da BitDefender para receber instruções ou tentar seguir procedimentos complicados, pode ver e seguir os passos apresentados nos tutoriais.

42.2. Pedir Ajuda

A secção **Resolução de Problemas e Obter Ajuda** providencia a informação necessária relativamente às incidências mais frequentes que poderá encontrar ao utilizar este produto.

Se não encontrar a solução para o seu problema nos recursos disponibilizados, pode contactar-nos directamente:

- "Contacte-nos Directamente Do Seu Produto BitDefender" (p. 255)
- "Contacte-nos através da nossa Base de Conhecimento Em Linha" (p. 256)

Importante

Para contactar o Apoio ao Cliente da BitDefender tem de ter a conta BitDefender activada.Para mais informação, por favor consulte o "*Registo e a Minha Conta*" (p. 55).

Contacte-nos Directamente Do Seu Produto BitDefender

Se possuir uma ligação activa à Internet, pode contactar o apoio do BitDefender directamente a partir do interface do produto (da janela do programa).

Para pedir ajuda, pode utilizar o Suporte Integrado disponível no produto.

Para utilizar o Suporte Integrado, siga os seguintes passos:

1. Abrir o BitDefender.
2. Clique na hiperligação **Ajuda e Suporte**, localizada no canto inferior direito da janela.
3. Agora tem duas opções:
   - Inicie uma procura na nossa base de dados para encontrar a informação que precisa.
   - Seleccione o departamento consoante o problema encontrado.

     Apoio ao cliente trata de questões de aquisições, licenças, reembolsos ou renovações.

     Apoio técnico inclui incidências relacionados com o próprio produto e respectiva operacionalidade.

     Luta contra malware aborda incidências relacionadas com vírus.
4. Leia os artigos ou os documentos e experimente as soluções propostas.
5. Se a solução não resolver o problema, utilize a hiperligação no artigo para iniciar a Ferramenta de Suporte.
6. Introduza o seu endereço electrónico, seleccione o departamento e escreva uma breve descrição do problema.

Clique **Seguinte**.

7. Por favor, aguarde alguns minutos enquanto o BitDefender recolhe as informações relacionadas com o produto. Esta informação irá ajudar os nossos engenheiros a encontrar uma solução para o seu problema.

   Clique **Seguinte**.

8. Clique em **Concluir** para enviar as informações ao Departamento de Apoio ao Cliente da BitDefender. Será contactado assim que possível.

Contacte-nos através da nossa Base de Conhecimento Em Linha

Se não conseguir aceder às informações necessárias com o produto BitDefender, por favor consulte a nossa base de conhecimento em linha:

1. Vá para http://www.bitdefender.com/help.A BitDefender Knowledge Base possui inúmeros artigos que contêm soluções para incidências relacionadas com o BitDefender.
2. Procure na BitDefender Knowledge Base os artigos que lhe poderão dar a solução para o seu problema.
3. Leia os artigos ou os documentos e experimente as soluções propostas.
4. Se a solução não resolver o problema, utilize a hiperligação no artigo para contactar o Apoio Técnico BitDefender.
5. Contacte o suporte BitDefender por e-mail, chat ou telefone.

43. Contactos

Comunicação eficiente é a chave de um negócio bem-sucedido. Durante os últimos 10 anos a BITDEFENDER estabeleceu uma reputação indiscutível ao exceder as expectativas dos clientes e parceiros, ao procurar constantemente melhorar a comunicação. Por favor não hesite em contactar-nos acerca de qualquer questão ou assunto que nos queira colocar.

43.1. Endereços Web

Departmento Comercial: comercial@bitdefender.pt
Suporte Técnico:www.bitdefender.com/help
Documentação: documentation@bitdefender.com
Programa de Parcerias: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Contactos Imprensa: pr@bitdefender.com
Oportunidades de Trabalho: jobs@bitdefender.com
Submeter Vírus: virus_submission@bitdefender.com
Submeter Spam: spam_submission@bitdefender.com
Relatórios de Abusos: abuse@bitdefender.com
Sítio de Internet do produto:http://www.bitdefender.com
Arquivos ftp do produto:ftp://ftp.bitdefender.com/pub
Distribuidores locais:http://www.bitdefender.com/site/Partnership/list/
Base de Conhecimento do BitDefender:http://kb.bitdefender.com

43.2. Distribuidores Locais

Os distribuidores locais BitDefender estão preparados para responder a quaisquer dúvidas relacionadas com as suas áreas de operação, quer sejam comerciais ou assuntos gerais.

Para encontrar um distribuidor BitDefender no seu país:

1. Vá para http://www.bitdefender.com/site/Partnership/list/.
2. A informação de contacto dos distribuidores locais BitDefender deve ser automaticamente apresentada. Se isto não acontecer, utilize o recurso de Localização de Parceiros no menu do lado esquerdo para seleccionar a área e o país de residência.
3. Se não encontrar um distribuidor BitDefender no seu país, não hesite em contactar-nos por correio electrónico através do endereço sales@bitdefender.com.Por favor, escreva a sua mensagem em inglês para podermos responder imediatamente.

43.3. Escritórios BitDefender

Os escritórios BitDefender estão preparados para responder a quaisquer perguntas respeitantes às suas áreas de operação, quer sejam questões comerciais e de assuntos gerais. Os seus respectivos endereços e contactos estão listados abaixo.

E.U.A.

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Telefone (office&sales): 1-954-776-6262
Vendas: sales@bitdefender.com
Suporte Técnico: http://www.bitdefender.com/help
Web: http://www.bitdefender.com

UK e Irlanda

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
Endereço electrónico: info@bitdefender.co.uk
Telefone: +44 (0) 8451-305096
Vendas: sales@bitdefender.co.uk
Suporte Técnico: http://www.bitdefender.com/help
Web: http://www.bitdefender.co.uk

Alemanha

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Escritório: +49 2301 91 84 222
Vendas: vertrieb@bitdefender.de
Suporte Técnico: http://kb.bitdefender.de
Web: http://www.bitdefender.de

Espanha

BitDefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
Fax: +34 93 217 91 28
Telefone: +34 902 19 07 65

Vendas: comercial@bitdefender.es
Suporte Técnico: www.bitdefender.es/ayuda
Website: http://www.bitdefender.es

Roménia

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefone Comercial: +40 21 2063470
E-mail Vendas: sales@bitdefender.ro
Suporte Técnico: http://www.bitdefender.ro/suport
Website: http://www.bitdefender.ro

44. Informações Úteis

Este capítulo apresenta alguns procedimentos importantes que tem de considerar antes de começar a fazer o diagnóstico de um problema técnico.

Resolver um problema técnico do BitDefender requer alguns conhecimentos do Windows, por isso os passos seguintes estão quase totalmente relacionados com o sistema operativo do Windows.

44.1. Como Posso Remover Outras Soluções de Segurança?

A principal razão para utilizar uma solução de segurança é proporcionar protecção e segurança aos seus dados.Mas o que acontece quando tem mais do que um produto de segurança no mesmo sistema?

Quando utiliza mais do que uma solução de segurança no mesmo computador, o sistema torna-se instável.O instalador do BitDefender Total Security 2011 detecta automaticamente outros programas de segurança e oferece-lhe a opção de os desinstalar.

Se não tiver removido as outras soluções de segurança durante a instalação inicial, siga os seguintes passos:

- Para o **Windows XP**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Adicionar/Remover Programas**.
  2. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
  3. Encontre o nome do programa que pretende remover e seleccione **Remover**.
  4. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.
- Para o **Windows Vista** e o **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
  2. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
  3. Encontre o nome do programa que pretende remover e seleccione **Desinstalar**.
  4. Aguarde que o processo de desinstalação termine, depois reinicie o seu sistema.

Se não conseguir remover as outras soluções de segurança do seu sistema, obtenha a ferramenta de desinstalação do sítio de Internet do fornecedor ou contacte-o directamente para receber instruções de desinstalação.

44.2. Como Posso Reiniciar no Modo de Segurança?

O Modo de Segurança é um modo operativo de diagnóstico, utilizado principalmente para detectar e resolver problemas que estejam a afectar o funcionamento normal do Windows.As causas destes problemas vão desde a incompatibilidade de controladores a vírus que impedem o arranque normal do Windows.No Modo de Segurança funcionam apenas algumas aplicações e o Windows só carrega os controladores básicos e os componentes mínimos do sistema operativo.É por isso que a maioria dos vírus está inactiva quando o Windows está no Modo de Segurança e podem ser facilmente removidos.

Para iniciar o Windows no Modo de Segurança:

1. Reinicie o computador.
2. Prima a tecla **F8** várias vezes antes de o Windows iniciar para aceder ao menu de arranque.
3. Seleccione **Modo de Segurança** no menu de arranque e prima **Enter**.
4. Aguarde enquanto o Windows é iniciado no Modo de Segurança.
5. Este processo termina com uma mensagem de confirmação.Clique em **Ok** para aceitar.
6. Para iniciar o Windows normalmente, basta reiniciar o sistema.

44.3. Estou a Utilizar uma Versão de 32 ou 64 Bit do Windows?

Para saber se tem um sistema operativo de 32 bit ou 64 bit, siga os seguintes passos:

- Para o **Windows XP**:
  1. Clique em **Iniciar**.
  2. Localize o **Meu Computador** no menu **Iniciar**.
  3. Clique com o botão direito em **Meu Computador** e seleccione **Propriedades**.
  4. Se estiver indicada a **Edição x64** na secção **Sistema**, está a executar a versão de 64 bit do Windows XP.

     Se não estiver indicada a **Edição x64**, está a executar a versão de 32 bit do Windows XP.
- Para o **Windows Vista** e o **Windows 7**:
  1. Clique em **Iniciar**.
  2. Localize o **Computador** no menu **Iniciar**.
  3. Clique com o botão direito em **Computador** e seleccione **Propriedades**.
  4. Procure na secção **Sistema** a informação sobre o seu sistema.

44.4. Como Posso Encontrar as Minhas Definições de Proxy?

Para encontrar estas definições, siga os seguintes passos:

- Para o Internet Explorer 8:
  1. Abra o Internet Explorer.
  2. Seleccione **Instrumentos** > **Opções de Internet**.
  3. No separador **Ligações** clique em **Definições LAN**.
  4. Na secção **Utilizar um servidor proxy para LAN** poderá encontrar p **Endereço** e a **Porta** do proxy.
- Para o Mozilla Firefox 3.6:
  1. Abra o Firefox.
  2. Seleccione **Instrumentos** > **Opções**.
  3. No separador **Avançadas**, abra o separador **Rede**.
  4. Clique em **Definições**.
- Para Opera 10.51:
  1. Abra o Opera.
  2. Seleccione **Recursos** > **Preferências**.
  3. No separador **Avançadas**, abra o separador **Rede**.
  4. Clique no botão **Servidores Proxy** para abrir a caixa de diálogo das definições proxy.

44.5. Como Posso Remover Totalmente o BitDefender?

Siga estes passos para remover correctamente o BitDefender:

1. Vá a www.bitdefender.com/uninstall e descarregue a ferramenta de desinstalação para o seu computador.
2. Execute a ferramenta de desinstalação com direitos de administrador.
3. Reinicie o seu computador.

44.6. Como Posso Activar/Desactivar a Protecção Em Tempo Real

O BitDefender providencia uma protecção contínua e em tempo-real, contra todo o tipo de ameaças de malware ao analisar os ficheiros acedidos, e as comunicações feitas através de aplicações de software de Mensagens Instantâneas (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Normalmente, a protecção em tempo real do BitDefender está activada e não deve ser desligada.

Quando tentar resolver um problema ou remover um vírus, poderá ter de desactivar a protecção em tempo real. Estes dizem respeito a uma das seguintes situações:

- Um problema de abrandamento com o sistema após a instalação do BitDefender
- Um problema com um programa ou uma aplicação após a instalação do BitDefender
- Mensagens de erro que poderão aparecer pouco depois da instalação do BitDefender

Siga os seguintes passos para poder activar/desactivar temporariamente a protecção em tempo real:

1. Abra o BitDefender, clique em **Opções** no canto superior direito da janela e escolha **Modo Avançado**.
2. Vá a **Antivirus** > **Escudo**.
3. Desmarque a caixa **A protecção em tempo real está activada** para desactivar temporariamente a protecção antivírus (ou seleccione-a se pretende activar a protecção).
4. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a protecção em tempo real.

Nota

Os passos para desactivar a protecção em tempo real no BitDefender devem ser utilizados como uma solução temporária e apenas durante um curto período.

44.7. Como Posso Mostrar Objectos Ocultos no Windows?

Estes passos são úteis nos casos de malware e tiver de encontrar e remover os ficheiros infectados, que poderão estar ocultos.

Siga os seguintes passos para mostrar objectos ocultos no Windows:

1. Clique em **Iniciar**, vá ao **Painel de Controlo** e seleccione **Opções de Pastas**.
2. Abra o separador **Ver**.
3. Seleccione **Mostrar conteúdo das pastas de sistema** (apenas para o Windows XP).
4. Seleccione **Mostrar ficheiros e pastas ocultos**.
5. Desmarque **Ocultar extensões de ficheiros nos tipos de ficheiro conhecidos**.
6. Desmarque **Ocultar ficheiros protegidos do sistema operativo**.
7. Clique em **Aplicar** e depois em **Ok**.

Glossário

ActiveX

O ActiveX é um modelo de escrita de programas, para que outros programas e o sistema operativo o possam chamar. A tecnologia do ActiveX é usada com o Microsoft Internet Explorer para criar páginas da Web interactivas, que parecem e compartam-se como programas de computador, em vez de páginas estácticas. Com o ActiveX, os utilizadores podem efectuar perguntas ou responder a questões, usando botões para carregar, e interagir de outras formas com a página da Web. Os controlos do ActiveX são frequentemente escritos utilizando o Visual Basic.

O Active X é notável para um leque completo de controlos de segurança; os especialistas de segurança dos computadores desencorajam o seu uso na Internet.

Adware

O adware é com frequência combinado com uma aplicação hospedeira que é fornecida sem custo desde que o utilizador concorde em aceitar o adware. Por causa de as aplicações adware serem normalmente instaladas após o utilizador concordar com uma licença de uso que define o propósito da aplicação, nenhuma ilegalidade é na verdade cometida.

No entanto, anúncios tipo pop-up podem tornar-se bastante incomodativos, e em alguns casos podem mesmo degradar a performance do sistema. Também, a informação que algumas dessas aplicações recolhem podem causar algumas preocupações de privacidade aos utilizadores que não estão completamente conscientes dos termos da licença de uso.

Arquivo

Um disco, cassete, ou directório que contém ficheiros que foram armazenados.

Um ficheiro que contém um ou mais ficheiros num formato comprimido.

Porta das traseiras

Um buraco na segurança de um sistema deliberadamente deixado ao acaso pelos desenhadores e protectores. A motivação para tais buracos não é sempre sinistra; alguns sistemas operativos, por exemplo, saem fora das caixas com contas priveligiadas, intencionadas para o uso no terreno por técnicos de serviço ou pelo vendedor dos programas de manutenção.

Sector de saída

Um sector no início de cada disco que identifica a arquitectura do disco (tamanho do sector, tamanho do grupo, e por aí a diante). Para discos de inicialização, o sector de saída também contém um progrma que carrega o sistema operativo.

Vírus de saída

Um vírus que infecta o sector de saída de um disco fixo ou de uma unidade de disquetes. A tentativa de retirar uma disquete infectada por um vírus de saída, irá causar a activação do vírus na memória. Sempre que iniciar o seu sistema daquele ponto, terá o vírus activo na memória.

Navegador

Diminuitivo para browser de internet, que é um software usado para localizar e mostrar páginas Web. Os dois mais populares browsers são o Netscape Navigator e o Microsoft Internet Explorer. Ambos são browsers gráficos, o que significa que eles tanto podem mostrar gráficos como texto. Em adição, a maioria dos browsers modernos podem apresentar informação multimédia, incluíndo som e vídeo, apesar de necessitarem de plug-ins para alguns formatos.

Linha de comando

Numa interface de linha do comando, o utilizador introduz comandos no espaço providenciado directamente no ecrã, usando a linguagem de comando.

Cookie

Desntro da indústria da Internet, as cookies são descritas como pequenos ficheiros, que contêm informação acerca de computadores individuais, que podem ser analizados e usados pelos publicitários para seguir o rasto online do seus interesses e gostos. Neste domínio, a tecnologia das cookies ainda está a ser desenvolvida e a sua intenção é encontrar alvos publicitários directamente do que disse serem os seus interesses. É uma espada de dois gumes para muitas pessoas, porque, por um lado aé eficiente e pertinente já que apenas vê anúncios do seu interesse. Por outro lado, envolve realmente "seguir o rasto" e "perseguir" onde vai e no que clica. Compreensivelmente, existe um debate acerca da privacidade e muitas pessoas sentem-se ofendidas ao terem a noção que estão a ser vistas como um "número SKU " (você sabe, o código de barras por detrás das embalagens que é verificado na mercearia). Enquanto este ponto de vista possa ser extremo, em alguns casos é preciso.

Componente (drive) do disco

É uma máquina que lê os dados do disco e escreve dados num disco.

Uma componente de disco rígido lê e escreve discos rígidos.

Uma componente de disquetes acede às disquetes.

As componentes do disco tanto podem ser internas (dentro do computador) ou externas (vêm numa caixa em separado que se liga ao computador).

Transferir

Para copiar dados (normalmente um ficheiro interno) de uma fonte principal para um aparelho periférico. O termo é frequentemente utilizado para descrever o processo de copiar um ficheiro de um serviço online para o seu próprio computador. Também se pode referir à cópia de um ficheiro de um servidor de ficheiros de rede, para um computador na rede.

Correio electrónico

Correio electrónico. É um serviço que envia mensagens em computadores via local ou redes globais.

Eventos

Uma acção ou ocorrência detectada por um programa. Os eventos podem ser acções do utilizador, tais como clicar no botão do rato ou carregar numa tecla, ou ocorrências do sistema, tais como ficar sem memórias.

Falso positivo

Ocorre quando o verificador identifica um ficheiro como infectado, quando na verdade ele não está.

Extensão do nome do ficheiro

A porção de um nome de ficheiro, que segue o ponto final, a qual indica o tipo de dados armazenados no ficheiro.

Muitos sistemas operativos usam extensões do nome do ficheiro, por ex. Unix, VMS, e MS-DOS. Elas são normalmente de uma a três letras. Os exemplos íncluem ".c" para C de código da fonte, ".ps" para PostEscrito, ".txt" para texto arbitrário.

Heurístico

Um método baseado na regra de identificar novos vírus. Este método de exame não se fia em assinaturas específicas de vírus. A vantagem do exame heurístico, é que não se deixa enganar por uma nova variante de um vírus existente. Contudo, pode reportar ocasionalmente códigos suspeitos em programas normais, gerando o chamado "falso positivo".

IP

Internet Protocol - Um rótulo de protocolo no protocolo TCP/IP séquito que é responsável dos endereços de IP, rotas, e a fragmentação e reabertura dos pacotes de IP.

Java applet

Um programa Java, o qual é desenhado para correr apenas numa página da web. Para usar uma applet numa página da web, you deverá especificar o nome da applet e o tamanho (comprimento e largura - em pixels) que a applet pode utilizar. Quando a página da web é acedida, o motor de busca descarrega a applet de um servidor e corre-a apenas na máquina do utilizador (o cliente). As applets diferem das aplicações, nas quais são administradas por um protocolo de segurança restrito.

Por exemplo, apesar de as applets correrem no cliente, elas não podem escrever nem lêr dados para a máquina do cliente. Adicionalmente, as applets são restritas para que possam apenas lêr e escrever dados provenientes do mesmo domínio, no qual elas são servidas.

Macro vírus

Um tipo de vírus de computador que está codificado como uma macro retido num documento. Muitas aplicações, tais como Microsoft Word e Excel, contêm poderosas linguagens macro.

Estas aplicações permitem-lhe reter uma macro num documento, e ter a macro pronta a ser executada sempre que o documento for aberto.

Cliente de mail

Um cliente de e-mail é uma aplicação que lhe permite enviar e receber e-mail.

Memória

Áreas internas de armazenamento no computador. O termo memória identifica armazenamento de dados que vêm na forma de chips, e a palavra armazenar é usada para a memória que existe em cassates ou discos. Todo o computador vem com uma certa quantidade de memótia física, normalmente referida como memória pricipal ou RAM.

Não-heurístico

Este método de exame confia em assinaturas de vírus especificas. A vantagem de um exame não-heurístico, é que ele não será induzido em erro pelo que possa parecer um vírus e não gera falsos alarmes.

Programas compactados

Um ficheiro num formato compactado. Muitos sistemas operativos e aplicações contêm comandos que lhe permitem compactar um ficheiro, para que ocupe menos memória. Por exemplo, suponha que tem um ficheiro de texto contendo dez espaços de caracteres consecutivos. Normalmente isto iria requerer dez de armazenamento.

Contudo, um programa que compacta ficheiros iria substituir o espaço dos caracteres por uma série-de-espaços de caracteres especial, seguida pelo número de espaços a ser substituidos. Neste caso, os dez espaços iriam requeres apenas dois bytes. Esta é apenas uma técnica de compactar, há muitas.

Caminho

As direcções exactas para um ficheiro num computador. Estas direcções são normalmente descritas por meios de preenchimento hierárquico do topo para baixo.

A rota entre dosi dados pontos, tal como os canais de comunicação entre dois.

Phishing

O acto de enviar um e-mail a um utilizador como sendo falsamente uma empresa legítima e estabelecida numa tentativa de levar o utilizador a providenciar informação privada que será utilizada para roubo. O e-mail leva o utilizador a visitar um site na Internet onde lhe é solicitado que actualize informação pessoa, tal como passwords e números de cartões de crédito, segurança social, e

números de contas bancárias, que a legítima organização já possui. O site Web, no entanto, é falso e está feito apenas para roubar a informação ao utilizador.

Vírus polimórfico

Um vírus que altera a sua forma com cada ficheiro que infecta. Dado que eles não têm uma consistência de patente binária, tais vírus são difíceis de identificar.

Porta

Uma interface num computador, à qual se liga um aparelho. Os computadores pessoais tendo vários tipos de portas. Internamente, existem várias portas para ligar componentes de disco, ecrãs, e tecladoss. Externamente, os computadores pessoais têm portas para ligar modems, impressoars, ratos, e outros aparelhos periféricos.

Nas redes TCP/IP e UDP, um ponto de fim para uma ligação lógica. O número da porta identifica o tipo da porta. Por exemplo, a porta 80 é usada para o tráfego HTTP.

Ficheiro de reporte

Um ficheiro que lista acções que tiveram ocurrência. O BitDefender um ficheiro de reporte que lista o caminho examinado, as pastas, o número de arquivos e ficheiros examinados, e quantos ficheiros suspeitos e infectados foram encontrados.

Rootkit

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

O papel principal dos rootkits é ocultar processos, ficheiros, logins e registos. Eles também podem interceptar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam ficheiros críticos usando rootkits. No entanto, eles são essencialmente utilizados para ocultar malware ou para esconder a presença de um intruso no sistema. Quando combinados com o malware, os rootkits são uma grande ameaça à integridade e segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar ficheiros e relatórios e evitarem ser detectados.

Escrita

Outro termo para macro ou ficheiro de porção, uma escrita é uma lista de comandos que podem ser executados sem a interacção do utilizador.

Spam

Lixo de correio electrónico ou lixo de avisos de newsgroups. É normalmente conhecido como correio não-solicitado.

Spyware

O estabelecimento de ligação à Internet do utilizador sem o seu conhecimento, normalmente para propósitos de publicidade. As aplicações de spyware são tipicamente adicionadas como um elemento oculto de programas freeware ou shareware que podem ser download a partir da Internet; no entanto salientamos que a maioria das aplicações freeware ou shareware não possuem spyware. Uma vez instalado, o spyware monitoriza a actividade do utilizador na Internet e transmite essa informação em background para alguém. O spyware pode também reunir informação acerca de endereços de e-mail e até mesmo passwords e números de cartões de crédito.

O spyware é similar a um cavalo-de-troia em que os utilizadores o instalam sem saberem, enquanto estão a instalar outra coisa qualquer. Uma forma comum de ser uma vítima de spyware é fazer download de determinado ficheiro peer-to-peer de produtos de swapping que se encontram actualmente disponíveis.

Para além destas questões de ética e privacidade, o spyware priva o utilizador de recursos de memória e também de largura de banda pois para enviar informação do utilizador para a fonte do spyware usa a ligação à Internet do utilizador. Por causa do spyware utilizar memória e recursos do sistema, as aplicações que estão a funcionar em background podem causar crashes no sistema ou uma grande instabilidade geral.

Itens que começam a funcionar ao ínicio

Qualquer ficheiro colocado nesta pasta, irá abrir quando o computador iniciar. Por exemplo, um ecrã que abra no ínicio, um ficheiro de som a ser tocado quando ligar inicialmente o computador, um lembrete, ou programas de aplicação podem ser itens que começam a funcionar ao iniciar o computador. Normalmente, é colocado um pseudónimo deste ficheiro nesta pasta, em vez do ficheiro em si próprio.

Caixa do sistema

Introduzido com o Windows 95, o tabuleiro do sistema está localizado na barra de tarefas do Windows (normalmente em baixo, junto ao relógio) e contém ícones em miniatura para um acesso fácil às funções do sistema, tais como fax, impressora, modem, volume, etc. Faça duplo-clique ou clique com o botão direito sobre o ícone para ver e aceder aos detalhes e controlos.

TCP/IP

Transmission Control Protocol/Internet Protocol - Um conjunto de protocolos de uma rede de trabalho abrangentemente usados Internet que permite comunicações ao londo de redes de computadores interconectadas com várias arquitecturas de hardware e vários sistemas operaticos. O TCP/IP ínclui padrões

de como os computadores comunicam e convenções para conectar redes e rotas de tráfego.

Tróiano

Um programa destrutivo que se mascara de aplicação benigna. Ao contrário dos vírus, os cavalos de Tróia não se replicam, mas podem ser tão destrutivos como os vírus. Um dos cavalos de Tróia mais incidente é o programa que promete ver-se livre dos vírus do seu computador, mas em vez disso introduz vírus no seu computador.

O termo provém de uma história da Ilíada de Homero, na qual os Gregos deram um cavalo gigante de Madeira aos seus inimigos, os Troianos, como uma oferta majestosa. Mas após os Troianos levarem o cavalo para dentro das muralhas da sua cidade, os soldados Gregos saíram para fora do cavalo e abriram os portões da cidade, permitindo que os seus compatriotas entrassem e dominassem Tróia.

Actualização

Uma nova versão de um produto de software ou hardware desenhada para substituir uma versão antiga do mesmo produto. Em adição, a instalação de rotina da actualização verifica se a versão anterior já está instalada no seu computador; se não estiver, não poderá instalar a actualização.

O BitDefender tem o seu próprio modulo de actualização que lhe permite verificar actualizações manualmente, ou permitir actualizar o produto automaticamente.

Vírus

Um programa ou um pedaço de código que é carregado no seu computador sem o seu conhecimento e decorre contra a sua vontade. A maioria dos vírus podem-se replicar. Todos os vírus de computação são feitos pelo Homem. Um simples vírus que se possa reproduzir a si próprio vezes sem conta, é relativamente fácil de fabricar. Mesmo um simples vírus é perigoso, porque usará rapidamente toda a memória disponível e levará o sistema a uma quebra. Ainda um mais perigoso tipo de vírus é aquele capaz de se transmitir ao longo das redes e ultrapassar sistemas de segurança.

Definição de vírus

A patente binária de um vírus, usada pelo programa de anti-vírus para detectar e eliminar os vírus.

Minhoca

Um programa que se propaga a si próprio ao longo de uma rede, reproduzindo-se à medida que avança. Não pode ligar-se sozinho a outros programas.